



PATRÍCIA ANDREIA BATISTA E SANTOS

A APLICAÇÃO DO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO LABORAL

Dissertação com vista à obtenção do grau de
Mestre em Direito e Gestão na especialidade de Proteção de Dados Pessoais

Orientador:

Doutor Francisco Pereira Coutinho, Professor na Faculdade de Direito da
Universidade Nova de Lisboa

Novembro 2019



PATRÍCIA ANDREIA BATISTA E SANTOS

A APLICAÇÃO DO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO LABORAL

Dissertação com vista à obtenção do grau de
Mestre em Direito e Gestão na especialidade de Proteção de Dados Pessoais

Orientador:

Doutor Francisco Pereira Coutinho, Professor na Faculdade de Direito da
Universidade Nova de Lisboa

Novembro 2019

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e de minha exclusiva autoria. Declaro ainda que todas as citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 28 de novembro de 2019

DECLARAÇÃO DE CONFORMIDADE DO NÚMERO DE CARACTERES

Declaro que o corpo da presente dissertação contém um total de 138 121 caracteres, incluindo espaços e notas de rodapé.

Declaro ainda que o resumo é constituído por 1 464 caracteres e o *abstract* por 1 397 caracteres, incluindo em ambos os espaços.

Lisboa, 28 de novembro de 2019

AGRADECIMENTOS

Após uma longa caminhada de muito trabalho, estudo e dedicação, quero agradecer a todas as pessoas que fizeram parte desta grande etapa da minha vida.

Em primeiro lugar, quero fazer um agradecimento especial ao Professor Doutor Francisco Pereira Coutinho por ter aceite orientar-me e ter dado todo o apoio que necessitei ao longo do desenvolvimento da dissertação, e, para além do mais, ter tido o privilégio de ser orientada por um professor por quem nutro uma grande admiração.

Agradeço também à Doutora Graça Canto Moniz pelo auxílio prestado durante todo o processo e a disponibilidade para debater alguns temas sobre a proteção de dados pessoais.

Em segundo lugar, agradeço as minhas amigas Beatriz, Cláudia e Inês, por terem-me “aturado” ao longo de todo o processo e ajudado quando mais precisei. E às minhas colegas Adriana, Ana, Daniela, Marisa, Rita e Vanessa por terem-me acompanhado não só nesta fase, mas durante todo o Mestrado, dando motivação para dar o meu melhor.

Agradeço também a toda a comunidade NOVA Direito desde funcionários, colegas e professores, pelo apoio que iam demonstrando até mesmo quando perguntavam “Como vai a tese?”.

Em terceiro lugar, mas não menos importante, aos meus pais, por terem-me apoiado em mais um capítulo da minha vida.

Obrigado a todos!

MODO DE CITAÇÃO E OUTROS ESCLARECIMENTOS

1. O modo de citação aplicado na presente dissertação segue o disposto das Normas Portuguesas n.º 405-1 e 405-4 do Instituto Português de Qualidade.
2. O modo de citação aplicado às monografias e publicações segue a seguinte forma: nome do autor, título da obra, edição, local, editora, ano e página. A partir da segunda referência apenas é referido o nome do autor, a indicação da nota onde foi mencionado pela primeira vez e a página. As Orientações do Grupo de Trabalho do Artigo 29.º e da Comissão Nacional de Proteção de Dados também segue esta última indicação.
3. As obras de pessoa coletiva seguem o mesmo modo de citação, porém apenas vai estar presente o nome de um dos autores com a indicação “*et al.*”.
4. As notícias e os *websites* consultados seguem a identificação do autor, título e o *link* associado com a data do seu acesso, estando estes elementos completos apenas na bibliografia final.
5. As expressões ou palavras de língua estrangeira são apresentadas em *itálico*.
6. Os textos em língua estrangeira foram traduzidos para a língua portuguesa. A tradução dos mesmos é da responsabilidade do autor.
7. A presente dissertação foi escrita ao abrigo do novo Acordo Ortográfico.

LISTA DE ABREVIATURAS

ACT – Autoridade para as Condições de Trabalho

AIPD – Avaliação de Impacto sobre a Proteção de Dados

Al. - Alínea

Art. – Artigo

CC – Código Civil

CdE – Conselho da Europa

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

Cit. - Citação

CNIL – *Commission Nationale de l'Informatique et des Libertés*

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

CV – *Curriculum Vitae*

Diretiva – Diretiva 95/46/CE

G29 ou GT – Grupo de Trabalho do Artigo 29.º

ICO – *Information Commissioner's Office*

N.º - Número

Para. - Parágrafo

P. - Página

RGPD ou Regulamento – Regulamento Geral de Proteção de Dados

RH – Recursos Humanos

TFUE – Tratado sobre o Funcionamento da União Europeia

TIC – Tecnologias de Informação e Comunicação

TJ ou TJUE – Tribunal de Justiça da União Europeia

UE – União Europeia

RESUMO

A entrada em vigor do Regulamento Geral de Proteção de Dados a 25 de maio de 2018, veio despertar a consciência dos titulares de dados através da informação que disponibilizam às empresas quando celebram algum tipo de contrato. Um exemplo disso, é o que sucede nas relações laborais.

O tratamento de dados pessoais no contexto laboral apresenta inúmeras matérias de estudo. Por ser uma área pouco discutida dentro do direito da proteção de dados pessoais, precisa de ser investigada para que, num futuro próximo, sirva de referência para compreender quais as implicações que o Regulamento representa para o tratamento de dados neste contexto. Assim, a presente dissertação dá a conhecer os tratamentos de dados efetuados dentro dos diferentes momentos do ciclo de vida do contrato de trabalho, em particular nos processos de recrutamento e celebração do contrato de trabalho.

Realça também as especificidades no tratamento, através dos fundamentos de legitimidade aplicados no vínculo laboral, destacando o papel do consentimento. Além disso, inclui a monitorização dos trabalhadores dentro e fora do local de trabalho, com enfoque no tratamento de dados biométricos e o regime do teletrabalho.

Em suma, pretende-se compreender como é aplicado o Regulamento nas relações laborais.

Palavras-chave: Regulamento Geral de Proteção de Dados; Relações laborais; Processos de recrutamento; Contrato de trabalho; Fundamentos de licitude; Monitorização dos trabalhadores

ABSTRACT

Since the General Data Protection Regulation, of 25th May 2018, has entered into force, it has awakened the conscience of data subjects who provide companies personal information when signing a contract. A great example of that often occurs within an employment relationship.

Personal data treatment in an employment relationship presents a variety of study cases. Since it is still a poorly discussed theme amidst data protection law, it needs to be properly studied, so that, in a nearby future, we might understand the implications that the new Regulation represents for personal data treatment within an employment relationship. Therefore, our essay allows us to explain how data treatment evolves within the circle of life of an employment agreement, most specifically in recruitment processes and employment contracts.

We will also mention some specificities on data treatment, referring to lawful basis for processing in employment relationships and highlighting the importance of consent. Moreover, we will discuss employee monitoring within or outside the workplace, focusing on biometric data processing and teleworking.

In essence, we aim to understand how the new Regulation will be applied in employment relationships.

Keywords: General Data Protection Regulation; Employment relationship; Recruitment process; Employment Contract; Lawful basis for processing; Employee Monitoring

INTRODUÇÃO

Os dados pessoais têm vindo a demonstrar ter um valor económico imprescindível, sobretudo desde o aparecimento das Tecnologias de Informação e Comunicação (TIC) entre as décadas de 60 e 70 do século passado. Após esse momento, a sociedade foi acompanhando a rápida ascensão tecnológica que deu origem a um novo mundo, no qual nos encontramos inseridos atualmente.

Este novo mundo denominado de “Sociedade da Informação”, é caracterizado por um conjunto de fatores associados à transformação tecnológica e às relações estabelecidas com a economia e a sociedade¹, dando origem à utilização de dados pessoais como “matéria-prima”, no sentido em que permitem atuar sobre a informação disponibilizada e não utilizar essa mesma informação para agir sobre as tecnologias, como acontecia anteriormente².

O rápido crescimento da tecnologia nos últimos anos e o surgimento da globalização trouxeram novos desafios para a proteção de dados pessoais no início do novo século. Consequentemente, a União Europeia (UE) iniciou uma reforma do regime jurídico da proteção de dados pessoais pela necessidade de ajustar o direito da proteção de dados aos desafios impostos pela sociedade, que se encontravam desatualizados através da Diretiva 95/46/CE³. Sendo neste contexto que surge o Regulamento Geral de Proteção de Dados (RGPD)⁴.

O RGPD veio devolver às pessoas o controlo sobre os seus dados pessoais, por serem cada vez mais valiosos para entidades públicas e privadas, dado o aumento

¹ WERTHEIN, Jorge - *A Sociedade da informação e os seus desafios*. In *Ciência de Informação*. Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia, Volume 9, n.º 2, 2000, p. 71-77. Disponível em <http://www.scielo.br/pdf/%0D/ci/v29n2/a09v29n2.pdf> (acedido a 02/07/2019).

² CASTELLS, Manuel - *A era da informação: economia, sociedade e cultura*. In *A Sociedade em rede*, 3ª edição. Lisboa: Fundação Calouste Gulbenkian, Volume 1, 2007, p. 87.

³ Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

⁴ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados).

significativo da recolha e partilha dos mesmos através da disponibilização pública e global por parte das pessoas singulares (considerando 6 do RGPD).

Neste sentido, ao devolver ao titular o controlo sobre os seus dados, vem despertar a consciência para salvaguardar os seus interesses, tendo em conta as informações que disponibiliza às empresas, de modo a resguardar a sua privacidade. Este controlo por parte do titular ocorre em qualquer contrato celebrado com uma empresa, devido ao valor atribuído pela utilização de dados pessoais. As relações laborais são um exemplo disso.

Durante um processo de recrutamento com vista a preencher uma vaga ou no momento em que o trabalhador exerce as suas funções, existe um conjunto de informações disponibilizadas por parte do titular em cada um dos momentos da relação laboral. Numa primeira fase, para dar a conhecer à empresa o seu potencial enquanto novo talento, e, na fase da contratação, as informações inerentes à execução do contrato e as obrigações jurídicas associadas ao mesmo.

Assim, vão surgindo as seguintes questões:

- 1) Qual será a finalidade do tratamento dos dados pessoais disponibilizados num processo de recrutamento?*
- 2) Que dados pessoais deve conter o Curriculum Vitae (CV)?*
- 3) Será que o recrutador/empregador consulta as redes sociais de possíveis candidatos/trabalhadores?*
- 4) Que dados estão a ser tratados na relação laboral?*

Estas questões são um exemplo das várias que devem ser colocadas quando o tratamento de dados pessoais envolve as relações laborais.

A presente dissertação tem como objeto investigar a aplicação do RGPD no contexto laboral, devendo-se esta escolha (i) pela novidade que o RGPD representa a nível europeu e nacional e (ii) ao debate sobre o tratamento de dados pessoais neste contexto em específico.

Em Portugal, as questões de âmbito laboral são pouco discutidas, sobretudo em temas relacionados com a proteção de dados pessoais, daí existir a necessidade de investigar este tema.

Optei por elaborar uma investigação generalizada, uma vez que o tratamento de dados neste contexto envolve várias matérias que necessitam ser exploradas para uma aplicação eficaz e completa do RGPD, considerando que se verificam inúmeras lacunas resultantes de a informação sobre as mesmas se encontrar dispersa e desatualizada.

Também se verificam algumas particularidades no tratamento de dados, neste contexto, que devem ser tidas em conta.

Através do presente trabalho de investigação, pretendo alcançar os seguintes objetivos:

- I. Perceber como o RGPD está a ser aplicado no contexto laboral;
- II. Transmitir, através da investigação, orientações para proceder ao tratamento de dados pessoais dos trabalhadores de uma forma mais direta; e
- III. Chamar a atenção para as especificidades de tratamento que devem ser tidas em conta no momento em que se inicia o ciclo de vida do contrato de trabalho.

O corpo da dissertação é composto por três capítulos, que apresentam três momentos distintos.

O 1.º Capítulo debruça-se sobre a proteção de dados pessoais na UE. Inicialmente, aborda a evolução histórica da proteção de dados pessoais a nível europeu e nacional, de forma a compreender a evolução desde os seus primórdios até aos dias de hoje, passando, de seguida, para o enquadramento do RGPD.

Como este apresenta inúmeros capítulos que cobrem todas as envolventes do direito da proteção de dados, apenas serão analisados os que apresentam uma ligação direta ao contexto laboral, fazendo um breve enquadramento de cada um deles com exceção dos conceitos, princípios relativos ao tratamento e direitos do titular de dados, que merecem uma especial atenção dada a sua relevância para a investigação.

O 2.º Capítulo apresenta o problema de investigação que incide no tratamento de dados pessoais no contexto laboral.

Este capítulo trata um vasto conjunto de situações que decorrem no tratamento de dados pessoais dos trabalhadores, estando assim divididos por cinco temas.

Em primeiro lugar, a introdução ao tema a partir do quadro legal relevante associado ao tratamento de dados pessoais no contexto laboral, dando um enfoque especial ao artigo 88.º do RGPD que trata estas questões.

De seguida, os fundamentos de legitimidade para o tratamento dos dados que constituem duas categorias específicas de tratamento, que tem suscitado dúvidas quanto à sua aplicação entre as várias autoridades de controlo europeias.

Em terceiro lugar, os tratamentos de dados que ocorrem no início da relação laboral através dos processos de recrutamento realizados em redes sociais profissionais – como o *LinkedIn* – e o método “tradicional” de entregar o CV e/ou preencher formulários de candidatura *online*, referindo ainda algumas situações particulares que ocorrem nestes processos através da aplicação de sistemas automatizados para auxiliar o recrutamento.

Dentro do ciclo de vida da relação laboral, o tema seguinte aborda uma questão discutida sempre que é mencionado o tratamento de dados pessoais no contrato de trabalho: se o consentimento constitui (ou não) um fundamento de licitude para o tratamento em âmbito laboral.

Por fim, a monitorização dos trabalhadores dentro e fora do local de trabalho, incidindo, sobretudo, em questões que não são discutidas quando abordada esta temática. Isto deve-se ao facto de serem situações recentes, que surgiram através dos desafios impostos pelas novas tecnologias e que, cada vez mais, são utilizadas neste contexto – o tratamento de dados biométricos para o controlo da assiduidade e o regime do teletrabalho.

O 3.º Capítulo, para finalizar, é constituído por um pequeno estudo de caso que tem por objeto compreender como o RGPD está a ser aplicado no seu primeiro ano de vigência relativamente ao exercício dos direitos de titulares de dados em candidatos a emprego, partindo da minha experiência enquanto candidata.

1.º CAPÍTULO – PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA

1.1 - A EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

Com o fim da Segunda Guerra Mundial, a Europa encontrava-se completamente devastada, enfrentando um período de grande instabilidade e reconstrução devido às perdas humanas e materiais sofridas durante essa época.

Para fazer face a esta situação, foi criado em 1949, o Conselho da Europa (CdE) com o objetivo de promover o Estado de Direito, a democracia e os direitos humanos⁵, prevenir as violações de direitos humanos verificadas durante a Guerra e dar resposta ao crescimento do comunismo na Europa Central e Oriental. A materialização deste objetivo encontra-se na Convenção Europeia dos Direitos do Homem (CEDH) que entrou em vigor em 1953⁶.

Nesta Convenção, encontra-se uma primeira referência, indireta, à proteção de dados pessoais, no artigo 8.º, que prevê o direito à vida privada e familiar, do seu domicílio e correspondência.

Esta primeira referência remete para o direito à privacidade, que foi adotado antes do aparecimento das novas tecnologias. Consequentemente, os desenvolvimentos desencadeados pela mesma, trouxeram vantagens para os indivíduos e para a sociedade em geral, mas também novos riscos associados ao direito à vida privada⁷.

No início dos anos 80, após o surgimento das TIC entre as décadas de 60 e 70, verificou-se a necessidade de desenvolver um novo enquadramento jurídico para a proteção de dados associado aos processos de automatização que estavam a surgir⁸. Assim, o CdE adotou em 1981, a Convenção para a Proteção dos Indivíduos face ao

⁵ SALDANHA, Nuno - *Novo Regulamento Geral da Proteção de Dados: O que é? A quem se aplica? Como implementar?*. Lisboa: FCA, 2018, p. 3.

⁶ Disponível em <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c> (acedido a 02/10/2018).

⁷ European Union Agency for Fundamental Rights, Council of Europe - *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018, p. 18.

⁸ DE HERT, Paul & LAMMERAN, Hans - *Protection of Personal Data in Work-related Relation – Study*. Brussels: European Parliament, 2013, p. 13.

Tratamento Automatizado de Dados Pessoais, conhecida como a Convenção 108, que visa garantir a todas as pessoas singulares o respeito pelos direitos e liberdades fundamentais, sobretudo, o direito à vida privada, face ao tratamento de dados automatizado. Este foi o primeiro instrumento internacional juridicamente vinculativo no domínio da proteção de dados⁹.

A Convenção 108 aplica-se ao tratamento de dados pessoais no setor público e privado, incluindo o tratamento realizado no âmbito da cooperação policial e judiciária em matéria penal e visa proteger os cidadãos contra os abusos que possam surgir com a recolha e tratamento de dados pessoais, tendo em conta o fluxo transfronteiriço de dados¹⁰.

Neste sentido, os princípios estabelecidos na Convenção 108 dizem respeito à recolha e tratamento automatizado de dados de forma lícita para finalidades determinadas e legítimas, utilizado apenas para fins compatíveis e conservados dentro do período necessário devendo os dados ser adequados, pertinentes e exatos.

Também apresenta garantias relativas ao tratamento de dados sensíveis, prevendo a proibição do seu tratamento na ausência de garantias jurídicas adequadas¹¹.

Nos anos 90, surgiu o primeiro instrumento jurídico de Direito da União Europeia relativo à proteção de dados: a Diretiva 95/46/CE e do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecida como a “Diretiva de Proteção de Dados”.

A aprovação da Diretiva deveu-se à necessidade de harmonizar um conjunto de leis nacionais, nesta matéria, que já estavam em vigor, garantindo um nível de proteção dos direitos e liberdades das pessoas singulares equivalente em todos os Estados-Membros, no que diz respeito ao tratamento de dados pessoais¹².

⁹ Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa - *Manual da Legislação Europeia sobre a Proteção de Dados*. Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 16.

¹⁰ *Idem.* p. 16.

¹¹ *Idem.* p. 18.

¹² *Idem.* p. 4.

Uma vez que os Estados-Membros eram partes contratantes da Convenção, a Diretiva desenvolveu os princípios gerais da Convenção 108, evitando-se contradições e aprofundando uma abordagem comum às normas, mas também criando novos instrumentos de proteção, como o caso das autoridades de controlo independentes¹³.

Posteriormente, o Tratado de Lisboa, veio reformar o enquadramento jurídico da proteção de dados pessoais da UE com a adoção do artigo 16.º do Tratado sobre o Funcionamento na União Europeia (TFUE) e dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

A Carta foi proclamada em 2000. Posteriormente, com a aprovação do Tratado de Lisboa, tornou-se juridicamente vinculativa como direito primário da UE, estabelecendo o direito à vida privada e familiar de todas as pessoas (art. 7.º do CDFUE) e o direito à proteção dos dados pessoais que lhe digam respeito, sendo objeto de tratamento lícito para finalidades específicas com o consentimento da pessoa em causa, assegurando o direito de aceder aos seus dados e obter a respetiva retificação (art. 8.º do CDFUE)¹⁴.

A entrada em vigor do Tratado de Lisboa (2009) e o relevo nele atribuído à proteção de dados pessoais, criam as condições para o desenvolvimento de um sistema mais eficaz de proteção de dados. Paralelamente, o desenvolvimento tecnológico criava riscos para os indivíduos que não encontravam proteção no diploma de 1995.

1.2 - A PROTEÇÃO DE DADOS PESSOAIS NA ORDEM JURÍDICA PORTUGUESA

Vivemos numa sociedade repleta de informação, impulsionada não só pela globalização, mas também pelo desenvolvimento das TIC nas últimas décadas. Neste sentido, o papel que as tecnologias da comunicação desempenham na vida socioeconómica, facilitando os fluxos de informação e métodos de trabalho, conduziu ao aparecimento de novos conflitos sociais.

¹³ DE HERT, Paul & LAMMERAN, Hans – Cit. 8, p. 14.

¹⁴ SALDANHA, Nuno - Cit. 5, p. 5.

A utilização indevida e ilícita da informação pode ser prejudicial para a vida íntima e privada dos envolvidos. As relações laborais não são exceção, com particulares especificidades tendo em conta o desequilíbrio de poderes e o grau de subordinação que resulta do contrato de trabalho¹⁵.

Deste modo, a sociedade começou a questionar se tínhamos o poder de conhecer e utilizar toda a informação de que dispomos, sobretudo se for relativa a terceiros podendo, de certo modo, a expor, tornando importante a definição de regras para proteger os dados pessoais¹⁶.

O direito à privacidade e o direito da proteção de dados, apesar de estarem relacionados e apresentarem valores similares, são direitos distintos¹⁷.

O direito à privacidade remete para situações que comprometam a vida privada de um indivíduo enquanto que o direito da proteção de dados ocorre no momento em que se verifica o tratamento de dados pessoais. Ou seja, são dois direitos que, de certo modo, acabam por estar correlacionados.

1.2.1 – A CONSTITUIÇÃO

A base jurídica do direito à privacidade encontra-se no artigo 26.º da Constituição da República Portuguesa (CRP) prevendo o reconhecimento a todos do direito à reserva da intimidade da vida familiar e privada (n.º 1), cabendo à lei estabelecer as garantias efetivas contra a obtenção e utilização abusiva ou contrária à dignidade humana, de informação relativa às pessoas e famílias (n.º 2).

Adicionalmente, o artigo 35.º da CRP garante a todos o direito ao acesso de dados informatizados que lhe digam respeito exigindo a sua retificação e atualização, como também o direito a conhecer a finalidade do tratamento dos dados (n.º 1), estabelecendo

¹⁵ SANTOS, Carlos - *Proteção de Dados dos Trabalhadores*. Lisboa: Universidade Autónoma de Lisboa, 2015, p. 13. Disponível em [repositorio.ual.pt/bitstream/11144/1856/1/Protecao de Dados dos Trabalhadores.pdf](https://repositorio.ual.pt/bitstream/11144/1856/1/Protecao%20de%20Dados%20dos%20Trabalhadores.pdf) (acedido a 19/02/2019).

¹⁶ *Idem*. p. 13.

¹⁷ European Union Agency for Fundamental Rights, Council of Europe – Cit. 7, p. 19.

que o tratamento de dados sensíveis apenas pode ser efetuado através do consentimento expresso do titular (n.º 3).

O artigo 35.º da CRP remete para os direitos dos titulares de dados pessoais previstos nos artigos 15.º e seguintes do RGPD.

1.2.2 – O CÓDIGO CIVIL

Além da CRP, o artigo 80.º do Código Civil (CC) apresenta o dever de guardar reserva quanto à intimidade da vida privada dos demais. Neste sentido, a teoria mais comum para delimitar o conteúdo do direito à privacidade e definir o conceito da reserva da intimidade da vida privada tem sido a “teoria das três esferas”¹⁸.

Esta teoria, de origem alemã, utilizada pela doutrina e jurisprudência portuguesa, é composta pela (i) esfera pública, a qual constitui toda a informação que deve e pode ser conhecida pelo público geral; a (ii) esfera privada, que contém informação apenas para um grupo restrito de pessoas; e (iii) a esfera íntima, em que a informação não é conhecida por outras pessoas, sendo vista como uma esfera “sagrada”¹⁹.

Assim, traça-se uma distinção através da natureza das informações partilhando-a em determinados grupos de dados pessoais dependendo do grau de proteção jurídica que acarreta cada esfera²⁰.

1.2.3 – O CÓDIGO DO TRABALHO

¹⁸ PRATA, Ana *et al.* - *Código Civil Anotado*. Coimbra: Edições Almedina, Volume 1, 2017, p. 120.

¹⁹ MARQUES, Garcia e MARTINS, Lourenço - *Direito da Informática*. Coimbra: Edições Almedina, 2000, p. 105.

²⁰ SANTOS, Carlos – Cit. 15, p. 15.

O Código do Trabalho (CT) prevê, no n.º 1 do artigo 16.º, que o empregador e trabalhador devem respeitar os direitos de personalidade²¹ da contraparte, guardando reserva quando à intimidade da vida privada²², sendo que esta abrange o acesso e a divulgação de aspetos referentes à vida íntima e pessoal das partes relativamente à vida familiar, afetiva e sexual, estado de saúde e convicções religiosas e políticas (n.º 2).

Verifica-se, então, que este artigo estabelece o princípio geral de todos os direitos de personalidade (n.º 1) especificando, no n.º 2, o direito à reserva da vida íntima e privada.

Ainda no CT, o n.º 1 do artigo 17.º estabelece que o empregador não pode exigir ao candidato a emprego e/ou trabalhador que preste informações relativas à sua vida privada, saúde e estado de gravidez, salvo quando seja estritamente necessário para o desenvolvimento da atividade profissional e execução do contrato.

Em qualquer caso, o candidato a emprego e/ou trabalhador que tenha fornecido informações de carácter pessoal tem o direito ao controlo dos seus dados pessoais, tendo o conhecimento da finalidade a que estes se destinam, podendo exigir a sua retificação e atualização (n.º 3 do presente artigo), tal como determina o n.º 1 do artigo 35.º da CRP e artigo 13.º do RGPD.

Neste sentido, devido à subordinação jurídica resultante do contrato de trabalho, há o risco de ocorrer um abuso da utilização de dados pessoais dos trabalhadores. Por isso, regra geral, o empregador não pode exigir ao trabalhador informações relativas à sua vida íntima e privada, salvo exceções em que seja permitida a recolha dessa informação por parte do empregador²³. Esta situação verifica-se pelo facto destas informações serem proibidas de tratar, devido à sensibilidade que acarretam esses dados pessoais.

²¹ Os direitos de personalidade são caracterizados como “aqueles sem os quais as pessoas não são tratadas enquanto pessoas, são direitos que são exigidos pela sua radical dignidade como e enquanto Pessoas Humanas, constituem fundamental ontológico da personalidade e da dignidade humana” (VASCONCELOS, Pedro Pais de - *Proteção de dados pessoais e direito à privacidade*. In *Direito da sociedade de informação I*. Coimbra: Coimbra Editora, 1999, cit. p. 249 - 250 sobre o enquadramento do direito à reserva da intimidade da vida privada como direito de personalidade.).

²² Neste contexto, influencia as disposições relativas a testes e exames médicos (art. 19.º), meios de vigilância (artigos 20.º e 21.º) e confidencialidade e acesso à informação (art. 22.º). Ver MARTINEZ, Pedro Romano *et al.* - *Código do Trabalho Anotado*, 11.º Edição. Coimbra: Edições Almedina, 2017, p. 152.

²³ O empregador só deve aceder a dados de carácter privado do trabalhador nos casos em que seja estritamente necessário e relevante para a execução do contrato. (ABRANTES, José João - *Direitos fundamentais da pessoa humana no trabalho em especial, a reserva da intimidade da vida privada (algumas questões)*. Coimbra: Edições Almedina, 2014, p. 27).

1.3 – O RGPD

1.3.1 – CONTEXTO DE APROVAÇÃO E OBJETIVOS

Em 2009, a Comissão Europeia iniciou a reforma da legislação de proteção de dados pessoais da UE através de duas comunicações: “*Uma abordagem global da proteção de dados pessoais na União Europeia*”, de 1 de novembro de 2010, e “*Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI*”, de 25 de janeiro de 2012.

A origem desta reforma deveu-se ao rápido crescimento da tecnologia e globalização que tem vindo a alterar profundamente a sociedade em que vivemos, trazendo novos desafios para a proteção de dados pessoais²⁴. Neste sentido, em 2010²⁵ verificou-se a necessidade de reformar e modernizar o regime jurídico da proteção de dados, por não responder aos desafios impostos pelas novas tecnologias, apesar de reconhecer a validade dos princípios fundamentais²⁶ da Diretiva.

Consequentemente, após um longo processo legislativo, iniciado em janeiro de 2012²⁷, foi publicado a 27 de abril de 2016, o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), que entrou em vigor a 25 de maio de 2018.

Entre os objetivos deste Regulamento, encontra-se o de contribuir para a modernização e harmonização da legislação de proteção de dados entre os Estados-Membros²⁸. Ou

²⁴ Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões «*Uma abordagem global da proteção de dados pessoais na União Europeia*», de 1 de novembro de 2010, p. 2.

²⁵ Ver Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões «*Uma abordagem global da proteção de dados pessoais na União Europeia*», de 1 de novembro de 2010.

²⁶ Os princípios da Diretiva baseiam-se na proteção dos direitos e liberdades fundamentais das pessoas singulares e a livre circulação de dados pessoais.

²⁷ European Union Agency for Fundamental Rights, Council of Europe – Cit. 7, p. 30.

²⁸ *Idem.* p. 30.

seja, ao ser um Regulamento e não uma Diretiva²⁹, não existe a necessidade de transpor para o ordenamento jurídico de cada Estado-Membro como acontecia anteriormente, conduzindo a um marco fundamental da sua reforma³⁰.

Adicionalmente, o RGPD surgiu como uma resposta ao atual estado do mundo, globalizado e tecnológico, constituindo um elemento crucial da Estratégia para o Mercado Único Digital³¹. O Mercado Único Digital apresenta o objetivo político da UE através da livre circulação de dados que deve seguir regras adaptadas, de forma a gerar a confiança necessária para desenvolver a economia digital em conjunto com o mercado interno (considerando 7 do RGPD).

Por outro lado, e tendo em conta os novos riscos tecnológicos para os indivíduos, o RGPD também visa reforçar o controlo dos indivíduos sobre os seus dados pessoais, por estes serem cada vez mais valiosos para empresas públicas e privadas, devido ao aumento significativo da recolha e partilha de dados pessoais, dada a sua disponibilização ser pública e global por parte das pessoas singulares (considerando 6 do RGPD).

Este controlo dos dados pessoais implica um reforço dos direitos dos titulares e a atribuição de responsabilidades a quem utiliza os dados, nomeadamente os “responsáveis pelo tratamento” ou “subcontratantes”. Em particular, o RGPD criou um conjunto de novas obrigações para estes sujeitos o que fez com que as empresas tivessem de reorganizar cuidadosamente os processos internos de proteção de dados de forma a estarem em conformidade com o RGPD³². No caso de incumprimento, podem enfrentar

²⁹ Existem diferenças quanto à aplicação de um Regulamento e uma Diretiva. O Regulamento é um ato legislativo vinculativo, aplicado em todos os seus elementos a todos os Estados-Membros, sem necessitar da intervenção das autoridades nacionais, ou seja, é diretamente aplicável. Já a Diretiva, é um ato legislativo que fixa um objetivo a atingir pelos Estados-Membros, sendo estes que elaboram a própria legislação para cumprir com esse objetivo. Disponível em https://europa.eu/european-union/eu-law/legal-acts_pt; <http://ccipd.pt/faqs/assuntos-europeus/> (acedido a 26/06/2019).

³⁰ European Union Agency for Fundamental Rights, Council of Europe – Cit. 7, p. 28 – 31.

³¹ Ver Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - *Estratégia para o Mercado Único Digital na Europa*, COM (2015) 192 final, Bruxelas, 6 de maio de 2015, p. 3. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> (acedido a 26/06/2019).

³² VOIGT, Paul & VON DEM BUSSCHE, Axel - *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Switzerland: Springer International Publishing AG, 2017, p. 2.

coimas até 20 000 000€ ou até 4% do volume de negócios anual (art. 83.º, n.º 5 do RGPD).

1.3.2 - PRINCIPAIS CONCEITOS

O artigo 4.º do RGPD elenca as diversas definições referentes às terminologias utilizadas ao longo do Regulamento. Vamos analisar aqueles que são mais revelantes para esta dissertação.

1) Dados Pessoais

Encontram-se definidos como “informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”)”. É “considerada identificável uma pessoa singular identificada, direta ou indiretamente, em especial por referência a um identificador” (n.º 1), tendo em atenção os meios suscetíveis de ser razoavelmente utilizados para identificar direta ou indiretamente a pessoa singular (considerando 26 do RGPD).

Estamos assim perante um conceito muito amplo³³, o que pode ser exemplificado por dois elementos daquela definição.

1. “Qualquer informação relativa a uma pessoa singular”

No Acórdão *Nowak*, o “emprego da expressão “qualquer informação” no âmbito da definição do conceito de “dado pessoal” (...) reflete o objetivo do legislador europeu de atribuir um sentido amplo a esse conceito, que não está limitado às informações sensíveis ou de ordem privada, mas engloba potencialmente qualquer tipo de informações, tanto objetivas como subjetivas sob forma de opiniões ou de apreciações, na condição de “dizerem respeito” à pessoa em causa”³⁴.

³³ No Acórdão *Google Spain*, verificou-se que a definição de dados pessoais apresentava uma definição muito ampla, pelo facto de existirem diversas situações associadas a esta definição, que dependem de caso para caso (Ver Acórdão de 13 de maio de 2014, “*Google Spain*”, C-131/12, ECLI:EU:C:2014:317, n.º 54).

³⁴ Acórdão de 20 de dezembro de 2017, “*Nowak*”, C-434/16, ECLI:EU:C:2017:994, n.º 34, cit.

Por norma, este conceito não é aplicado a pessoas coletivas. Mas no Acórdão *Volker und Schecke e Eifert*, o TJUE veio referir que “as pessoas coletivas só podem invocar a proteção dos artigos 7.º e 8.º da CDFUE (...) desde que a denominação legal da pessoa coletiva identifique uma ou mais pessoas singulares”³⁵. O mesmo acontece quando aplicado a pessoas falecidas (considerando 27 do RGPD).

2. “Informação relativa a uma pessoa singular identificada ou identificável”

A identificação não é imediata, mas existe a probabilidade razoável do titular poder ser identificado futuramente por quem trata a informação ou por terceiros (considerando 26 do RGPD). Por exemplo, através de imagens gravadas em vídeo, registos de tempos de trabalho, entre outros.

Nesta definição cabem as categorias especiais de dados, isto é, dados que revelem a “origem racial ou étnica, as opiniões públicas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos (...) dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa”, por isso, em regra, o seu tratamento é proibido (n.º 1 do art. 9.º do RGPD).

Não obstante, nas relações laborais existem situações específicas em que é aplicado o tratamento de categorias especiais de dados por estas constituírem uma obrigação legal no vínculo contratual, como vamos verificar no 2.º capítulo.

2) Tratamento

É “uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição” (n.º 2).

³⁵ Acórdão de 9 de Novembro de 2010, “*Volker und Schecke e Eifert*”, C-92/09 e C-93/09, ECLI:EU:C:2010:662, n.º 53, cit.

Um exemplo claro de uma operação de tratamento é o que sucede nos processos de recrutamento em que os dados tratados são todos aqueles que constam do CV e do formulário de candidatura, ou, no caso de ser através das redes sociais profissionais, dos dados que se encontram no perfil profissional do candidato.

3) Definição de perfis

Consiste em “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações” (n.º 4).

Este conceito é relevante na medida em que o titular, segundo o artigo 22.º e considerando 71 e 72 do RGPD, tem o direito de não ficar sujeito a uma decisão que se baseie exclusivamente no tratamento automatizado produzindo efeitos na sua esfera jurídica ou que o afete significativamente.

Em particular, verifica-se o crescente recurso, por parte das empresas, a sistemas automatizados para auxiliar os processos de recrutamento com o intuito de selecionar, com maior precisão, o candidato ideal para preencher a vaga disponível através da análise do seu perfil comportamental e profissional.

Neste sentido, o responsável pelo tratamento tem o dever de informar sobre a existência de definição de perfis e informações relativas a essa definição, de forma a compreender como o algoritmo chega àquela conclusão (artigos 13.º, n.º 2, al. f); 14.º, n.º 2, al. f) e 15.º, n.º 1, al. h) do RGPD), apesar de isso ser tecnicamente muito difícil. Deve ser realizada uma avaliação de impacto sobre a proteção de dados (AIPD), quando se verifique este tipo de tratamentos (al. a), n.º 3 do art. 35.º do RGPD).

4) Responsável pelo tratamento e Subcontratante

Responsável pelo tratamento	Subcontratante
“Pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais” (n.º 7 e considerando 81 do RGPD)	“Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento” (n.º 8 e considerando 82 do RGPD)

O legislador europeu atribui diferentes graus de responsabilidade a estes dois sujeitos. No caso do responsável pelo tratamento, recaem sobre ele todas as obrigações do RGPD; no caso do subcontratante, recaem apenas algumas obrigações que serão analisadas mais adiante.

A existência de um subcontratante depende da decisão do responsável pelo tratamento de externalizar o tratamento. Por exemplo, quando uma empresa recorre a uma empresa de trabalho temporário para recrutar novos trabalhadores, essa empresa é o subcontratante e a de trabalho temporário o responsável pelo tratamento. Todavia, existe uma grande dificuldade na aplicação prática destas figuras, devido à distribuição dos seus papéis num ambiente de grande complexidade, em que podem ocorrer vários cenários que envolvam múltiplos responsáveis pelo tratamento e subcontratantes. Desta forma, são essenciais os Pareceres do Grupo de Trabalho do Artigo 29.º (G29)³⁶ para entender as funções de cada um.

Com o RGPD, a subcontratação passou a ter novos e mais exigentes requisitos. Assim, segundo o artigo 28.º:

³⁶ Como o exemplo do Grupo de Trabalho do Artigo 29.º - *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, adotado em 16 fevereiro de 2010.

1. O “responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes” de forma a assegurar a “defesa dos direitos do titular dos dados”;
2. O “subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização”;
3. A subcontratação é regulada por um contrato, contendo os elementos mencionados no n.º 3;
4. A Comissão (n.º 7) e a autoridade de controlo (n.º 8) podem estabelecer cláusulas contratuais-tipo.

1.3.3 – PRINCÍPIOS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS

Os princípios relativos ao tratamento de dados pessoais (art. 5.º do RGPD) são considerados uma chave de leitura do RGPD estando concretizados noutras disposições, em especial, nas obrigações que recaem sobre os responsáveis pelo tratamento, bem como nos direitos do titular de dados.

1) Princípio da licitude, lealdade e transparência

De acordo com este princípio, os dados pessoais são “objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados” (al. a) do n.º 1 do art.º 5 do RGPD). Este princípio tem como principais concretizações, as (i) condições de licitude (art. 6.º do RGPD), as (ii) categorias especiais de dados (art. 9.º do RGPD) e o (iii) dever de informar relacionado com os direitos do titular dos dados (artigos 12.º e seguintes do RGPD).

I. Condições de licitude

Trata-se do fundamento que o responsável pelo tratamento deve apresentar para o tratamento dos dados pessoais. Assim, o tratamento só é lícito, por exemplo, se o titular tiver dado o consentimento (al. a) do n.º 1 do art. 5.º do RGPD).

Além do consentimento, há outras condições de licitude: (i) o contrato de trabalho onde este fundamenta o tratamento de informações relativas ao processamento salarial; (ii) em diligências pré-contratuais, no caso de solicitar a uma seguradora uma proposta e esta poder tratar os dados necessários para fundamentar a proposta; (iii) uma obrigação jurídica³⁷, apesar de não ser necessário o consentimento por poder recair sobre o responsável pelo tratamento; e (iv) no interesse legítimo³⁸ do responsável pelo tratamento, sobretudo, quando há uma relação com o titular dos dados.

II. Categorias especiais de dados

Como já foi mencionado, por norma, é proibido o tratamento de categorias especiais de dados (n.º 1 do art. 9.º do RGPD). Todavia, existem situações particulares no âmbito laboral que fogem à regra, como o tratamento para efeitos do cumprimento de obrigações e do exercício de direitos específicos associados à relação laboral e testes e exames médicos (alíneas b) e h) do n.º 2 do art. 9.º do RGPD), como vamos verificar mais adiante.

III. O dever de informar

Sem entrar em grande detalhe dado que os direitos do titular dos dados são tratados ao longo do ponto 1.3.4, é importante mencionar que surgiram novos direitos do titular através do RGPD (direito à portabilidade (art. 20.º)) e outros foram sendo reconhecidos através de decisões do TJUE (direito ao esquecimento (art. 17.º)).

2) Princípio da limitação da finalidade

Este princípio é fundamental por ser aquele que define a realização do tratamento de dados pessoais. Ou seja, quando os dados vão ser tratados, o titular tem o direito de saber qual é a finalidade, de forma a consentir (ou não) o tratamento dos dados³⁹.

³⁷ No Acórdão *Worten*, verificou-se a obrigação do empregador disponibilizar à Autoridade das Condições de Trabalho o acesso imediato do registo dos tempos de trabalho (n.º 1 do art. 202.º do CT). (Ver Acórdão de 30 de maio de 2013, “*Worten*”, C-342/12, ECLI:EU:C:2013:355, n.º 15).

³⁸ É uma situação que pode ocorrer em situações em que o titular é cliente e para efeitos de comercialização direta (considerando 47 do RGPD).

³⁹ PINHEIRO, Alexandre Sousa - *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. Lisboa: AAFDL, 2015, p. 826.

Portanto, os dados são recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com essas finalidades (al. a) do n.º 1 do art. 5.º do RGPD). Assim, assume duas dimensões – a determinação da finalidade do tratamento e a utilização compatível com a finalidade⁴⁰.

Mas existem situações em que o tratamento poderá ser realizado posteriormente, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos (al. b) do n.º 1 do art. 5.º do RGPD).

Existem disposições no RGPD articuladas com este princípio, como é o caso da obrigação de criar um registo de todas as atividades de tratamento prevendo a finalidade do tratamento dos dados (al. b) do n.º 1 do art. 30.º).

O Parecer do GT 3/2013 refere a possibilidade, dependendo de caso para caso, da existência de flexibilidade na aplicação deste princípio⁴¹, o que sucede, por exemplo, em lojas de pequena dimensão. Estas não precisam de especificar a finalidade de tratamento de forma detalhada como uma loja de grande dimensão que utiliza esses mesmos dados para personalizar ofertas e publicidade dirigida aos seus clientes.

3) Princípio da minimização

Os dados pessoais são “adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados” (al. c) do n.º 1 do art. 5.º do RGPD). É um princípio novo, dado que anteriormente estava implícito no princípio da proporcionalidade.

Segundo este princípio, é necessário que os dados sejam limitados ao mínimo, sendo apenas tratados se a finalidade do tratamento não puder ser atingida de forma razoável através de outros meios⁴².

⁴⁰ Grupo de Trabalho do Artigo 29.º - *Parecer 3/2013 sobre a limitação da finalidade*, adotado em 2 de abril de 2013. p. 6.

⁴¹ *Idem*. p. 18.

⁴² PINHEIRO, Alexandre Sousa *et al.* - *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 209.

As principais concretizações verificam-se através da proteção de dados desde a conceção e por defeito (art. 25.º do RGPD), dos prazos de conservação (al. e) do n.º 1 do art. 5.º do RGPD) e no direito ao apagamento (art. 17.º do RGPD).

4) Princípio da exatidão

Os dados pessoais são exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (al. d) do n.º 1 do art. 5.º do RGPD).

Este princípio está relacionado com o direito de retificação (art. 16.º do RGPD) e com o apagamento dos dados (art. 17.º do RGPD).

5) Princípio da conservação

Os dados pessoais são conservados de uma forma que permita a identificação dos titulares apenas durante o período necessário para as finalidades para as quais são tratados. Os dados podem ser conservados durante longos períodos, desde que sejam tratados exclusivamente para fins de arquivo, interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (al. e) do n.º 1 do art. 5.º do RGPD).

A sua concretização poderá levar a prazos de retenção ou apagamento dos dados. De forma a assegurar que sejam conservados durante o período necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou revisão periódica (considerando 39 do RGPD).

6) Princípio da integridade e confidencialidade

Os dados pessoais são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas e organizativas adequadas (al. f) do n.º 1 do art. 5.º do RGPD).

A sua concretização encontra-se nas normas relacionadas com a segurança dos dados pessoais através da adoção de medidas de prevenção (art. 32.º do RGPD) de violações de dados pessoais e procedimentos de reação às mesmas, como as notificações e comunicações de violações de dados pessoais (artigos 33.º e 34.º do RGPD).

7) Princípio da responsabilidade

Exige dos responsáveis pelo tratamento a adoção de medidas que garantam o respeito dos princípios e obrigações do RGPD e, quando solicitado, a demonstração da conformidade às autoridades de controlo. Este princípio surgiu através do Parecer do GT 3/2010.

Com a implementação do RGPD, o legislador europeu mudou a abordagem relativamente às exigências de responsabilidade por parte do responsável pelo tratamento, conduzindo a um paradigma regulatório previsto no considerando 89 do RGPD.

Anteriormente, era necessário consultar a autoridade de controlo para aprovar determinado tratamento de dados pessoais. Só que o legislador entendeu que esta obrigação originava encargos administrativos e financeiros que nem sempre contribuíam para a melhoria da proteção de dados, porque a maior parte das empresas não consultava a autoridade de controlo antes de iniciar o tratamento, demonstrando que este modelo estava a falhar.

Assim, foi substituído por regras e procedimentos internos aplicados pelo responsável pelo tratamento devendo refletir as medidas tomadas para proteger os dados pessoais. Consequentemente, a autoridade de controlo é substituída pelo responsável pelo tratamento, que passa a ter a responsabilidade de garantir que os dados estão seguros no seio da empresa.

Dada a responsabilidade atribuída ao responsável pelo tratamento, este deve seguir as obrigações previstas no artigo 24.º do RGPD. Entre elas, a obrigação de gerir adequadamente os riscos que decorrem do tratamento, que podem afetar os direitos e

liberdades das pessoas singulares, sendo estes identificados, analisados, estimados, avaliados, tratados e revistos regularmente⁴³.

1.3.4 – DIREITOS DO TITULAR DE DADOS PESSOAIS

O objetivo fundamental do RGPD consiste em garantir a aplicação prática da proteção de dados dando algum controlo ao titular sobre os seus dados pessoais. Assim, o legislador europeu tentou encontrar uma forma de garantir o exercício prático desses direitos através dos direitos do titular de dados (artigos 12.º e seguintes do RGPD), como já acontecia anteriormente com a Diretiva.

1) Direito de acesso

É caracterizado como o direito “mãe” por ser o principal direito do titular dos dados⁴⁴. Isto porque quando um titular pretende exercer algum direito sobre os seus dados pessoais tem de saber que dados possui o responsável pelo tratamento.

Portanto, o titular tem o direito de obter do responsável pelo tratamento a confirmação de que os dados são objeto de tratamento e, se for o caso, de aceder aos mesmos (n.º 1 do art. 15.º do RGPD).

O direito de acesso acaba por estar ligado ao direito de informação (artigos 13.º e 14.º do RGPD)⁴⁵ impondo um conjunto de obrigações ao responsável através da obtenção de informações específicas sobre o tratamento efetuado (alíneas a) a h) do n.º 1 do art. 15.º do RGPD). Assim, o efeito do seu exercício é obter do responsável uma

⁴³ Grupo de Trabalho do Artigo 29.º - *Orientações relativas à Avaliação de Impacto sobre a Proteção de dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, revistas e adotadas em 4 de outubro de 2017. p. 7.

⁴⁴ O direito de acesso está previsto no n.º 1 do artigo 35.º da CRP, elencando os direitos de retificação e atualização e o direito ao conhecimento da finalidade da recolha e tratamento. (PINHEIRO, Alexandre Sousa *et al.* – Cit. 42, p. 357).

⁴⁵ Os artigos 13.º e 14.º do RGPD são mais densos e exigentes em relação à Diretiva. (Ver HENRIQUES, Sérgio Coimbra e LUÍS, João Vares - *Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*. In PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.) - *Anuário da Proteção de Dados 2019*. Lisboa: CEDIS, 2019, p. 23).

cópia sobre os dados pessoais (n.º 3 do art. 15.º do RGPD), a qual deve conter as informações elencadas no n.º 1 do artigo 13.º do RGPD.

É um direito que não apresenta exceções, tirando os direitos e as liberdades de terceiros⁴⁶ (n.º 4 do art. 15.º e considerando 63 do RGPD).

2) Direito de oposição

Quando se fala do direito de oposição, é necessário fazer a distinção entre tratamentos lícitos e ilícitos de dados pessoais. Esta distinção deve-se ao facto de o tratamento de dados pessoais se basear no interesse legítimo do responsável pelo tratamento, por este resultar de uma obrigação legal.

Na prática, o titular vai pedir ao responsável pelo tratamento a ponderação entre os seus próprios interesses e o interesse do titular relativamente ao tratamento dos dados pessoais de forma a que o titular possa, a qualquer momento, opor-se ao tratamento dos seus dados (n.º 1 do art. 21.º do RGPD).

Quando exercido este direito, os dados serão apagados por não existir outro fundamento que justifique o seu tratamento. Todavia, se existirem razões imperiosas e legítimas para o tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular, o direito de oposição não pode ser exercido.

Assim, o seu efeito é baseado no apagamento dos dados por não existir outro fundamento legítimo para a conservação dos dados pessoais.

3) Direito a não ser avaliado com base em tratamento automático

Pode ser visto como um direito especial de oposição, por atribuir ao titular dos dados o direito de não ficar sujeito a decisões tomadas exclusivamente por tratamentos automatizados de dados, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente (n.º 1 do art. 22.º do RGPD).

⁴⁶ O exercício do direito de acesso não prejudica os direitos e liberdades de terceiros. Porém, não devem recusar a prestação de todas as informações dadas ao titular dos dados quando este obtém uma cópia dos dados pessoais. (PINHEIRO, Alexandre Sousa *et al.* – Cit. 42, p. 362).

O considerando 71 do RGPD apresenta alguns exemplos desse tipo de processos como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem intervenção humana. Ou seja, o titular pode exercer este direito referindo que não quer ser avaliado com base em tratamentos automatizados. Consequentemente, o efeito é a proibição de decisões tomadas exclusivamente com base em tratamento automatizado.

Todavia, é uma obrigação do responsável pelo tratamento de não proceder a este tipo de avaliação. Portanto, não se configura como um direito, mas sim como uma obrigação do responsável, podendo ser caracterizado como um direito de oposição especial para os casos em que se verifique este tipo de situações.

Este direito apresenta algumas exceções relativamente a decisões necessárias para: (i) celebração ou execução de um contrato entre o titular e o responsável pelo tratamento; (ii) autorizada pelo direito da União ou do Estado-Membro; e (iii) baseada no consentimento explícito do titular dos dados (n.º 2 do art. 22.º).

4) Trilogia de direitos do titular

A trilogia de direitos do titular tem o objetivo de responder a patologias no tratamento de dados pessoais sendo composta pelo direito à retificação, apagamento e limitação de tratamento.

4.1- Direito de retificação

Apresenta o direito de retificar, sem demora, os dados pessoais inexatos que digam respeito ao titular, demonstrando a possibilidade de serem completados, tendo em conta as finalidades do tratamento (art. 16.º do RGPD). Por conseguinte, os dados pessoais devem ser retificados ou completados pelo responsável pelo tratamento. É um direito que está associado ao princípio da exatidão.

O artigo 19.º do RGPD apresenta uma disposição de salvaguarda, pelo facto de a retificação ser comunicada a cada terceiro destinatário dos dados, salvo se essa

comunicação for impossível ou implicar um esforço desproporcionado. Poderá vir a ter alguma aplicação em ambientes digitais, onde ocorra a comunicação de dados pessoais.

4.2– Direito ao apagamento / Direito a ser esquecido

É um direito de dupla qualificação (apagamento/a ser esquecido) que traduz a utilização dos dois nomes como se fossem sinónimos da mesma coisa. Porém, não é isso que acontece.

O direito ao apagamento (n.º 1 do art. 17.º do RGPD) não tem tanta relevância como muitos entendem, pelo facto de o direito de oposição conduzir ao apagamento dos dados pessoais.

Verifica-se quando os dados pessoais deixam de ser necessários para a finalidade que levou à recolha: a retirada do consentimento; a oposição do tratamento; o tratamento ilícito; o apagamento dos dados para o cumprimento de uma obrigação jurídica; e dados pessoais tratados no contexto da oferta de serviços da sociedade da informação (al. a) a f) do n.º 1 do presente artigo) – sendo esse o seu efeito, a eliminação dos dados.

O legislador europeu preocupou-se em prever um conjunto alargado de situações em que não autoriza o apagamento dos dados pessoais. Assim, apresenta uma limitação ao direito de apagar os dados, por estes estarem associados ao interesse público (n.º 3 do art. 17.º do RGPD).

Através do efeito do exercício do direito ao apagamento, surge o direito ao esquecimento.

Este direito conduz não só ao apagamento no ambiente digital como à desindexação da informação. Foi reconhecido no Acórdão *Google Spain*⁴⁷.

⁴⁷ Mario Costeja González tinha uma dívida à Segurança Social espanhola que foi executada, conduzindo à publicação dessa informação através do jornal “*La Vanguardia*”. Porém, a versão digital do jornal manteve essa informação, mesmo após González ter saldado a dívida, levando a que o seu nome aparecesse sempre associado à dívida quando pesquisado no motor de busca da *Google*.

Descontente com a situação, González solicitou a um tribunal espanhol, chegando mais tarde ao TJUE, que a *Google* fosse obrigada a desindexar essa informação. Assim, o TJUE veio a reconhecer o direito ao esquecimento nos motores de busca (“*Google Spain*”, C-131/12, ECLI:EU:C:2014:317).

Neste sentido, o titular pode solicitar ao responsável pelo tratamento o apagamento dos dados, quando este os tornar públicos e for obrigado a apagá-los, devendo informar os restantes responsáveis que o titular solicitou a desindexação para esses dados, como das cópias e reproduções dos mesmos, tomando as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da aplicação (n.º 2 do art. 17.º do RGPD).

4.3 – Direito à limitação do tratamento

É o direito que confere ao responsável pelo tratamento a obrigação de colocar os dados pessoais em “quarentena”, enquanto aguarda por uma decisão final do que fazer em relação a eles, a pedido do titular dos dados.

Prevê que o titular possa impor a limitação do tratamento dos dados nos casos em que contesta a exatidão dos dados pessoais; o tratamento for ilícito e se opuser ao apagamento e solicitar, em contrapartida, a limitação; o responsável já não precisar dos dados, mas estes serem necessários para efeitos do exercício de um direito no processo judicial; e se tiver oposto ao tratamento, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados (alíneas a) a d) do n.º 1 do artigo 18.º do RGPD).

O efeito do seu exercício remete para a cessação do tratamento dos dados através do responsável pelo tratamento; o exercício de um direito num processo judicial; a salvaguarda de um interesse público relevante e a proteção de direitos de terceiros (n.º 2 do art. 18.º do RGPD). A exceção é a conservação dos dados por estes já se encontrarem limitados.

5) Direito à portabilidade

É um novo direito que surgiu com o RGPD. Apresenta uma dimensão mais política do que propriamente jurídica, dada a transmissão de dados pessoais entre responsáveis pelo tratamento ser efetuada sempre que tal seja tecnicamente possível (n.º 2 do artigo 20.º e considerando 68 do RGPD).

É uma situação que vai depender dos meios técnicos que os responsáveis pelo tratamento disponham, apresentando um formato interoperável que permita a portabilidade.

Neste sentido, o titular deve ter o controlo sobre os seus dados. Portanto, ao exercer o direito à portabilidade, tem o direito de receber uma cópia dos dados que tinha fornecido ao responsável pelo tratamento (n.º 1 do artigo 20.º do RGPD). Ou seja, pode ser visto como um direito de acesso, visto que o titular tem uma cópia dos dados pessoais, estando este associado ao exercício da portabilidade entre responsáveis, por ser essa cópia igualmente transmitida entre os responsáveis pelo tratamento.

O exercício do direito à portabilidade apenas pode ser efetuado quando o tratamento dos dados se basear no consentimento ou num contrato e for realizado por meios automatizados (alíneas a) e b) do n.º 1 do art. 20.º do RGPD).

6) Direito de resposta

Quando o titular dos dados exerce algum dos direitos previstos nos artigos 15.º a 20.º do RGPD, o responsável pelo tratamento deve, sem demora injustificada e no prazo de um mês a contar da data da receção do pedido, fornecer as informações sobre as medidas tomadas no exercício desses direitos. No entanto, o prazo pode ser prorrogado até dois meses, pela complexidade e o número de pedidos (n.º 3 do art. 12.º do RGPD). O mesmo sucede quando o responsável pelo tratamento não der seguimento ao pedido efetuado pelo titular (n.º 4 do presente artigo).

As comunicações entre o responsável pelo tratamento e o titular dos dados, relacionadas com o exercício dos direitos devem ser fornecidas gratuitamente. Não obstante, em casos de pedidos manifestamente infundados ou excessivos, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos ou a recusar o seguimento ao pedido (n.º 5 do art. 12.º do RGPD).

1.3.5 – OS PAPÉIS DO RESPONSÁVEL PELO TRATAMENTO E DO SUBCONTRATANTE

O artigo 24.º do RGPD apresenta uma disposição relativa às responsabilidades do responsável pelo tratamento, reforçando o seu papel através do n.º 2 do artigo 5.º do RGPD.

Entretanto, o G29 emitiu no Parecer 3/2010 as exigências relativas aos responsáveis pelo tratamento através da aplicação de medidas adequadas e eficazes de forma a garantir o respeito dos princípios e obrigações do RGPD e, quando solicitado, a demonstração às autoridades de controlo⁴⁸.

O considerando 89 do RGPD estabelece a obrigação geral de notificar o tratamento dos dados às autoridades de controlo, sendo que essas obrigações deverão ser substituídas por regras e procedimentos eficazes e mais centrados em operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares.

Assim, para compensar a ausência de intervenção prévia da autoridade de controlo, o legislador europeu impôs aos responsáveis pelo tratamento e subcontratantes um vasto conjunto de novas obrigações.

Como se verificou no ponto 1.3.2, recai sobre o responsável pelo tratamento todas as obrigações do RGPD, assumindo desta forma o princípio da responsabilidade.

Obrigações do Responsável pelo Tratamento	
Obrigação de gestão adequada do risco	Incide na concretização do princípio da responsabilidade, questionando o risco associado a uma empresa. Assim, quando apresenta um maior risco do tratamento de dados pessoais, mais exigente se torna. Isto porque, a empresa acarreta uma maior responsabilidade, como mais obrigações são impostas ao responsável pelo tratamento (n.º 1 do art. 24.º do RGPD).

⁴⁸ Grupo de Trabalho do Artigo 29.º - *Parecer 3/2010 sobre o princípio da responsabilidade*, adotado em 13 de julho de 2010. p. 4.

Identificação e documentação do fundamento do tratamento	<p>É uma exigência do princípio da licitude que vai depender das finalidades do tratamento de dados casuisticamente (art. 5.º do RGPD).</p> <p>Coima: al. a) do n.º 5 do artigo 83.º do RGPD</p>
Direitos do titular de dados pessoais	<p>O responsável pelo tratamento facilita o exercício dos direitos do titular dos dados (n.º 2 do art. 12.º do RGPD), respeitando um conjunto de regras gerais e específicas associadas ao seu exercício.</p> <p>Coima: al. b) do n.º 5 do artigo 83.º do RGPD</p>
Escolha do subcontratante	<p>Encontra-se prevista no artigo 28.º do RGPD elencando os seguintes requisitos: apresentar “garantias suficientes de execução de medidas técnicas e organizativas adequadas”, por exemplo, códigos de conduta ou certificação (n.º 1 e 4); um regime imperativo do contrato de subcontratação (n.º 2); cláusulas contratuais-tipo estabelecidas pela comissão ou autoridade de controlo (n.º 7 e 8); e o contrato por escrito.</p> <p>Coima: al. a) do n.º 4 do artigo 83.º do RGPD</p>
Registo das atividades de tratamento de dados pessoais	<p>O registo das atividades de tratamento deve conter informações relativas ao responsável pelo tratamento e, quando se verifique, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados (al. a) do n.º 1 do art. 30.º do RGPD).</p> <p>Os limites estabelecidos ao registo de atividades de tratamento incidem no n.º 5 do presente artigo.</p> <p>Coima: al. a) do n.º 4 do artigo 83.º do RGPD</p>
Proteção de dados desde a conceção e por defeito	<p>Segundo o artigo 25.º do RGPD, as medidas devem ser implementadas desde a conceção, no momento de definição dos meios e do próprio tratamento e, por defeito, quando os dados são necessários para a finalidade específica do tratamento.</p> <p>Coima: al. a) do n.º 4 do artigo 83.º do RGPD</p>
Segurança do tratamento e Notificação de violação de dados pessoais	<p>Segundo o n.º 12 do artigo 4.º do RGPD, uma violação de segurança pode provocar, “de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento”.</p> <p>Para que situações dessa natureza não aconteçam, os artigos 32.º e seguintes do RGPD indicam as obrigações que recaem sobre os utilizadores de dados pessoais através da prevenção de violações de dados pessoais (art. 32.º), a notificação de uma violação de dados à autoridade de controlo (art. 33.º) e a comunicação da mesma ao titular quando apresenta um elevado risco (art. 34.º).</p> <p>Coima: n.º 4 e 5 do artigo 83.º do RGPD</p>
Avaliação de impacto e Consulta prévia	<p>Os procedimentos específicos da avaliação de impacto e consulta prévia encontram-se previstos nos artigos 35.º e 36.º do RGPD. É obrigatório realizar uma avaliação de impacto quando a operação de tratamento apresente um elevado risco para os direitos e liberdades das pessoas singulares (n.º 1 do art. 35.º do RGPD) como ocorre nas situações previstas no n.º 3 do presente artigo.</p> <p>A lista das operações de tratamento sujeitas ao requisito de avaliação de impacto é elaborada e tornada pública pela autoridade de controlo (n.º 4 do art. 35.º do RGPD).</p> <p>Coima: al. a) do n.º 4 do artigo 83.º do RGPD</p>

Transferência de dados pessoais fora da UE	Quando ocorre a transferência de dados pessoais para um país terceiro ou organização internacional, é aplicado o regime das transferências regulado pelos artigos 44.º e seguintes do RGPD. Coima: al. c) do n.º 5 do artigo 83.º do RGPD
Encarregado de Proteção de Dados	O encarregado de proteção de dados apenas é obrigatório nas situações mencionadas no n.º 1 do artigo 37.º do RGPD. Assim, o responsável pelo tratamento e o subcontratante asseguram que este é envolvido nas questões relacionadas com a proteção de dados (art. 38.º do RGPD). Coima: al. a) do n.º 4 do artigo 83.º do RGPD

O subcontratante assume novas obrigações que estão interligadas às do responsável pelo tratamento, garantindo a conformidade com o RGPD.

Obrigações do Subcontratante	
Colaboração com a Autoridade de Controlo	O artigo 31.º do RGPD prevê a colaboração da CNPD com o responsável pelo tratamento e subcontratante e, em caso disso, com os seus representantes. Coima: al. a) do n.º 4 do artigo 83.º do RGPD
Notificar o responsável pelo tratamento no caso de ocorrer uma violação dos dados	O subcontratante notifica o responsável pelo tratamento, e não a autoridade de controlo, quando tem conhecimento de uma violação de dados (n.º 2 do art. 33.º do RGPD). Coima: al. a) do n.º 4 do artigo 83.º do RGPD
Registo das atividades de tratamento e Encarregado de Proteção de Dados	Aplicam-se, de igual modo, ao subcontratante como ao responsável pelo tratamento.

Além das obrigações, o subcontratante celebra um contrato de forma a estar vinculado ao responsável pelo tratamento, estabelecendo o objeto, duração, natureza e finalidade do tratamento, o tipo de dados e as categorias dos titulares de dados, e as obrigações e direitos do responsável pelo tratamento (n.º 3 do art. 28.º do RGPD).

1.3.6 – AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

A AIPD é um processo que decorre quando um certo tipo de tratamento utiliza, sobretudo, novas tecnologias e tendo em conta a natureza, âmbito, contexto e finalidade presente um elevado risco para os direitos e liberdades das pessoas singulares. É realizada pelo responsável pelo tratamento, antes de iniciar a operação de tratamento (n.º 1 do art. 35.º do RGPD).

Deve incluir as medidas, garantias e procedimentos para atenuar os riscos e assegurar o cumprimento do RGPD (considerando 90 do RGPD). Assim, é realizada do seguinte modo (n.º 7 do art. 35.º do RGPD):



Figura 1 – Processo de Avaliação de Impacto sobre a Proteção de Dados⁴⁹

Através da figura, verifica-se que a AIPD é composta por três fases distintas – descritiva, avaliativa e decisória.

A primeira fase descreve as operações de tratamento previstas e a sua finalidade e, caso se verifique, os interesses legítimos do responsável pelo tratamento.

⁴⁹ Fonte: Grupo de Trabalho do Artigo 29.º - Cit. 43, p. 19.

A segunda apresenta duas dimensões: a avaliação relacional entre as operações de tratamento e os objetivos ligados ao princípio da proporcionalidade e a avaliação dos riscos para os direitos e liberdades dos titulares.

A terceira assenta nas medidas para atenuar os riscos (garantias, medidas de segurança e procedimentos destinados para assegurar o cumprimento do RGPD)⁵⁰.

A AIPD é obrigatória nos casos em que ocorra: (i) tratamento automatizado de dados, incluindo definição de perfis, que levem a uma avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, produzindo efeitos jurídicos e afetando significativamente o titular; (ii) operações de tratamento em grande escala de categorias especiais de dados ou de dados relacionados com condenações penais e infrações; e (iii) controlo sistemático de zonas acessíveis ao público em grande escala (n.º 3 do art. 35.º do RGPD).

Mas também deve ser tido em conta as situações em que se verifique que não é necessário realizar uma AIPD⁵¹.

Após a avaliação, se esta indicar que o tratamento apresenta um elevado risco com ausência de medidas tomadas pelo responsável pelo tratamento, este não poderá atenuar o risco, e assim, terá que consultar a autoridade de controlo antes de proceder ao tratamento de dados pessoais (n.º 1 do art. 36.º e considerando 94 do RGPD).

Neste sentido, a autoridade de controlo elabora e torna pública uma lista com os tipos de tratamento que necessitam de realizar uma AIPD⁵². Mas também pode fazer o mesmo relativamente aos tipos de tratamento em que não é obrigatório realizá-la, sendo ambas as listas comunicadas ao Comité (n.º 4 e 5 do art. 35.º do RGPD).

⁵⁰ PINHEIRO, Alexandre Sousa *et al.* – Cit. 42, p. 461.

⁵¹ O G29 elenca um conjunto de situações em que não é obrigatório realizar uma AIPD, sendo todas aquelas que não apresentem um risco elevado para os direitos e liberdades das pessoas singulares. (Ver Grupo de Trabalho do Artigo 29.º - Cit. 43, p. 15).

⁵² A CNPD apresenta o *Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD-DPIA)*, de 16 de outubro de 2018.

Ao longo do 2.º Capítulo, iremos verificar que existem várias situações de tratamento em que é necessário realizar uma AIPD, sobretudo as que envolvam a monitorização dos trabalhadores dentro e fora do local de trabalho.

1.3.7 – AUTORIDADE DE CONTROLO

A autoridade de controlo⁵³ tem como responsabilidade fiscalizar a aplicação do RGPD, de forma a defender os direitos e liberdades das pessoas singulares relativamente ao tratamento e facilitar a circulação desses dados na UE, podendo ser estabelecidas uma ou mais autoridades públicas independentes (n.º 1 do art. 51.º do RGPD). Apresenta o dever de cooperação, no sentido de cooperar com as autoridades de controlo europeias e com a Comissão, quando se verifique essa necessidade (n.º 2 do art. 51.º e art. 60.º e seguintes do RGPD).

É-lhe atribuída um vasto conjunto de obrigações, sendo apresentadas as que possuem um maior grau de importância (n.º 1 do art. 57.º do RGPD):

- Sensibilização (al. b) e d)), aconselhamento (al. c)), informação (al. e)), acompanhamento de novas tecnologias (al. i)), orientação (al. l)), incentivos à elaboração de códigos de conduta (al. m)) e ao estabelecimento de procedimentos de certificação, selos e marcas de proteção de dados (al. n));
- Cooperação a nível internacional (alíneas f), g) e h));
- Adotação de cláusulas contratuais-tipo para contratos entre o responsável pelo tratamento e subcontratante para a transferência de dados pessoais para países terceiros (al. j));

⁵³ A CNPD é a autoridade de controlo nacional, de carácter administrativo independente, que controla e fiscaliza o processamento de dados pessoais, respeitando os direitos consagrados na Constituição e na lei. Também coopera com as autoridades de controlo de outros Estados-Membros, relativamente na defesa e no exercício dos direitos dos indivíduos residentes em países terceiros. Disponível em <https://www.cnpd.pt/bin/cnpd/acnpd.htm> (acedido a 15/11/2018).

- Elaboração e conservação de uma listagem de tratamentos sujeitos a AIPD (al. k));
- Autorização de cláusulas contratuais e disposições previstas no n.º 3 do artigo 46.º do RGPD; e
- Aprovação de regras vinculativas aplicáveis às empresas (al. s)).

Além das atribuições, é composta por três poderes - investigação, correção e consultivos e de autorização (art. 58.º do RGPD).

O poder de investigação (n.º 1) implica: o fornecimento de informação necessária pelo responsável pelo tratamento e subcontratante (al. a)); a realização de auditorias (al. b)); a obtenção do acesso a todos os dados pessoais e informações necessárias (al. e)), bem como as instalações, equipamentos e meios de tratamento por parte do responsável pelo tratamento e subcontratante (al. f)).

O poder de correção (n.º 2) remete para: a indicação de advertências (al. a)) e repreensões ao responsável pelo tratamento e subcontratante (al. b)); ordenar a comunicação ao titular dos dados (al. e)), bem como a suspensão do envio de dados para países terceiros (al. j)); imposição de limitações temporárias ou proibição de tratamentos de dados (al. f)); e aplicação de coimas (al. i)).

Os poderes consultivos e de autorização (n.º 3) referem-se ao aconselhamento do responsável pelo tratamento no âmbito do procedimento de consulta prévia prevista na alínea a) do presente artigo e artigo 36.º do RGPD; a aprovação de códigos de conduta (al. d)); e acreditação de organismos de certificação (al. e)).

No 3.º Capítulo, analisaremos o modo de atuação da autoridade de controlo nacional perante a apresentação de uma queixa pelo incumprimento dos direitos de titulares de dados, neste caso, o direito de acesso.

2.º CAPÍTULO – TRATAMENTO DE DADOS PESSOAIS NO CONTEXTO LABORAL

2.1 – ENQUADRAMENTO

Analizando a atividade laboral de uma empresa relativamente ao tratamento de dados pessoais, verifica-se que a sua composição se baseia no ciclo de vida do contrato de trabalho. No entanto, os dados pessoais não são tratados apenas quando ocorre o vínculo laboral, mas também numa fase pré-contratual, de recrutamento, de contratação propriamente dita, bem como na fase da cessação da relação laboral.

No contexto da atividade laboral, o tratamento de dados pessoais deve ser situado num destes três momentos, de modo a enquadrar a legislação aplicável a cada um. Porém, podem ocorrer situações específicas, nas quais é necessário aplicar regulamentação especial, como sucede nos contratos de trabalho temporário⁵⁴.

No que ao RGPD diz respeito, o mesmo dispõe, no artigo 88.º, a possibilidade de os Estados-Membros estabelecerem no seu ordenamento jurídico ou em convenções coletivas⁵⁵, normas mais específicas para garantir a defesa dos direitos e liberdades relativamente ao tratamento de dados pessoais dos trabalhadores (primeira parte do n.º 1).

Ou seja, com o poder que o RGPD atribui ao legislador nacional, o tratamento de dados neste contexto, deve ser articulado com o artigo 28.º da Lei n.º 58/2019⁵⁶, de forma a assegurar ao empregador o tratamento de dados pessoais dos trabalhadores seguindo as normas do CT, a legislação complementar e outros regimes setoriais, com as

⁵⁴ O contrato de trabalho temporário é composto por uma relação tripartida entre a empresa de trabalho temporário, o utilizador e o trabalhador. Através desta relação, o utilizador apresenta obrigações inerentes à subordinação jurídica repartidas com a empresa de trabalho temporário. Assim, durante a execução do contrato, o poder de direção é atribuído ao utilizador e o poder disciplinar à empresa de trabalho temporário (art. 185.º, n.º 2 e 4 do CT). Desta forma, a empresa de trabalho temporário é o responsável pelo tratamento, pelo facto de as suas obrigações jurídicas estarem ligadas ao tratamento de dados – processamento salarial e documentos com dados pessoais. (PINHEIRO, Alexandre Sousa *et al.* – Cit. 42, p. 671 e 672).

⁵⁵ Em Portugal, não sabemos se as convenções coletivas irão incorporar normas mais específicas por estas terem uma origem contratual.

⁵⁶ Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

especificidades que constam no presente artigo (n.º 1 do presente artigo), abrangendo igualmente o tratamento de dados efetuado pelo subcontratante ou contabilista certificado, para efeitos da gestão de recursos humanos, desde que seja realizado ao abrigo de um contrato de prestação de serviços (n.º 2).

As finalidades de tratamento previstas são todas aquelas que se encontram associadas às relações laborais. Deste modo, produzem efeitos: (i) no recrutamento; (ii) execução de contrato; (iii) gestão, planeamento e organização do trabalho; (iv) igualdade e diversidade do local de trabalho; (v) saúde e segurança no trabalho; (vi) proteção dos bens do empregador ou do cliente; (vii) exercício e gozo dos direitos e benefícios relacionados com o emprego; e (viii) cessação do contrato (segunda parte do n.º 1 do art. 88.º do RGPD).

Neste sentido, de forma a garantir a conformidade do tratamento, o responsável deve adotar medidas adequadas e específicas para salvaguardar a dignidade, interesses legítimos e os direitos fundamentais do titular, com especial atenção à transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e sistemas de controlo no local de trabalho (n.º 2 do art. 88.º do RGPD).

Além desta peça legislativa, o CT elenca várias normas remissivas (artigos 16.º e seguintes) que tratam as questões de âmbito laboral, estando estas descritas no ponto 1.2.3 do 1.º Capítulo.

Por fim, é importante considerar a legislação avulsa respeitante a estas matérias ou que regulam algumas atividades como o caso da Lei n.º 102/2009⁵⁷ e o Decreto-lei n.º 260/2009⁵⁸.

Além da legislação mencionada, as orientações do Comité Europeu para a Proteção de Dados (CEPD)⁵⁹ são fundamentais para compreender as situações

⁵⁷ Regime Jurídico da Segurança e Saúde no Trabalho (Lei n.º 102/2009, de 10 de setembro republicada pela Lei n.º 3/2014 de 28 de janeiro).

⁵⁸ Regime do exercício e licenciamento da atividade da empresa de trabalho temporário e do acesso e exercício da atividade da agência privada de colocação de candidatos a emprego (Decreto-lei n.º 260/2009, republicado pela Lei n.º 5/2014 de 12 de fevereiro e alterado pela Lei n.º 146/2015).

⁵⁹ O G29 deixou de existir com a entrada em vigor do Regulamento, passando o Comité Europeu para a Proteção de Dados a assumir as suas funções (artigos 68.º e seguintes do RGPD).

específicas de tratamento designadamente, o Parecer 2/2017 sobre o tratamento de dados pessoais no local de trabalho⁶⁰.

Este parecer completa questões tratadas em orientações anteriores⁶¹, refletindo uma “nova avaliação do equilíbrio entre o interesse legítimo dos empregadores e a expectativa razoável de privacidade dos empregados”⁶² de forma a demonstrar as preocupações inerentes às alterações verificadas no local de trabalho com o desenvolvimento das novas tecnologias.

Após uma breve alusão ao tema em análise, as seguintes matérias vão incidir nos diferentes tratamentos de dados pessoais que ocorrem nas relações laborais.

2.2 – OS FUNDAMENTOS DE LICITUDE

Os dados pessoais no âmbito laboral são todos aqueles que englobam o trabalhador – desde o recrutamento à cessação do contrato – e o seu desenvolvimento – passando pela gestão do talento.

No entanto, as normas do RGPD não apresentam, de forma expressa, os fundamentos de legitimidade para o tratamento de dados pessoais dos trabalhadores⁶³. Com efeito, estes fundamentos encontram-se dispersos ao longo do mesmo, designadamente nos artigos 6.º e 9.º.

Apesar disso, a constituição dos fundamentos de licitude remete para duas categorias distintas que resultam da diferente categorização de dados pessoais a serem tratados. Deste modo, são compostos pelas categorias de dados (art. 6.º do RGPD) e categorias especiais de dados (art. 9.º, n.º 2 do RGPD).

⁶⁰ Grupo de Trabalho do Artigo 29.º - *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*, adotado em 8 de junho de 2017.

⁶¹ Grupo de Trabalho do Artigo 29.º - *Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral* e o *documento de trabalho de 2002 sobre a vigilância das comunicações eletrónicas no local de trabalho*.

⁶² Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 4, cit.

⁶³ HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – Cit. 45, p. 21.

As categorias de dados referem-se à: (i) execução do contrato; (ii) obrigação jurídica; e aos (iii) interesses legítimos do responsável pelo tratamento⁶⁴ ou de terceiros⁶⁵ previstos nas alíneas b), c) e f) do n.º 1 do artigo 6.º do RGPD.

I. Execução de contrato

Este fundamento tem sido descrito como sendo “essencial” no contexto do tratamento de dados dos trabalhadores, sendo o mais utilizado pelo empregador⁶⁶.

II. Obrigação jurídica⁶⁷

Encontra-se associada ao tratamento de dados pessoais para efeitos da gestão de recursos humanos - como o processamento salarial - e às obrigações impostas pela legislação laboral ao empregador, designadamente obrigações em matéria de segurança e saúde no trabalho, por exemplo⁶⁸.

III. Interesses legítimos

São vistos como um fundamento de licitude especialmente exigente no RGPD, por obrigar a fazer uma ponderação entre esse interesse e os riscos que o tratamento implica para o titular dos dados. Ou seja, o empregador ao invocar o interesse legítimo deverá, desde logo, verificar se a finalidade a que se destina o tratamento é legítima. Adicionalmente, deve tomar medidas que garantam o equilíbrio necessário entre a finalidade para o tratamento de dados e o respeito pelas liberdades e direitos fundamentais do titular e as expectativas razoáveis do mesmo⁶⁹.

Um exemplo da aplicação dos fundamentos de legitimidade previstos no artigo 6.º do RGPD, é o tratamento de dados da avaliação de desempenho e progressão na carreira.

⁶⁴ Neste contexto, o responsável pelo tratamento é o empregador.

⁶⁵ Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 7.

⁶⁶ HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – Cit. 45, p. 30 – 31.

⁶⁷ Quando o tratamento de dados é realizado em conformidade com uma obrigação jurídica que o responsável pelo tratamento esteja sujeito, esse tratamento deverá ser regulado através do direito da União ou de um Estado-Membro. Daí poder resultar uma lei para as diversas operações de tratamento baseadas neste fundamento (considerando 45 do RGPD).

⁶⁸ HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – Cit. 45, p. 28 – 29.

⁶⁹ *Idem.* p. 31.

Pode ser visto como execução de contrato, mas também pode ser interesse legítimo por parte do responsável pelo tratamento. É uma situação que vai depender não só do quadro contratual em causa, como da perspectiva do trabalhador e do empregador.

Quanto às categorias especiais de dados, o n.º 1 do artigo 9.º do RGPD proíbe o tratamento destes dados, admitindo-o no contexto laboral, segundo as exceções do n.º 2, sendo apenas tratados os dados referentes à filiação sindical, dados relativos à saúde e dados biométricos para o controlo da assiduidade e acesso. A alínea b) e h) deste artigo demonstram um contexto específico, na medida em que estes foram desenhados para a realidade laboral, estando associados ao cumprimento de obrigações e exercício de direitos específicos relacionados à relação laboral e a testes e exames médicos.

Após identificados os fundamentos de licitude, surge a seguinte dúvida relativamente à sua aplicação:

- *Neste contexto apenas é aplicado o artigo 6.º do RGPD e quando se trata de uma categoria especial de dados o artigo 9.º, n.º 2 do RGPD, ou será que os dois artigos são aplicados cumulativamente?*

Segundo a Autoridade para as Condições de Trabalho (ACT)⁷⁰, a legitimidade para o tratamento dos dados baseia-se na execução do contrato e no cumprimento de uma obrigação jurídica (alíneas b) e c) do n.º 1 do art. 6.º do RGPD), que pode depender de legislação complementar ou outros regimes setoriais. O mesmo se verifica relativamente às categorias especiais de dados através do cumprimento de obrigações e do exercício de direitos específicos associados à relação laboral (al. b) do n.º 2 do art. 9.º do RGPD).

Mas não refere como os fundamentos de licitude são aplicados, apenas menciona quais são.

⁷⁰ Nota técnica n.º 8 da ACT - *Impacto do Regulamento Geral de Proteção de Dados nas relações laborais*. Disponível em [http://www.act.gov.pt/\(pt-PT\)/Publicacoes/Documents/Nota%20T%C3%A9cnica%20n%C2%BA%208%20-%20Impacto%20do%20Regulamento%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20nas%20Rela%C3%A7%C3%B5es%20Laborais.pdf](http://www.act.gov.pt/(pt-PT)/Publicacoes/Documents/Nota%20T%C3%A9cnica%20n%C2%BA%208%20-%20Impacto%20do%20Regulamento%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20nas%20Rela%C3%A7%C3%B5es%20Laborais.pdf) (acedido a 17/05/2019).

Ao pensar de forma lógica, o artigo 6.º do RGPD prevê como fundamento de licitude a execução de um contrato. Ou seja, em regra geral, o artigo 6.º do RGPD é aplicado pelo facto da relação laboral traduzir na celebração do contrato entre trabalhador e empregador, destacando assim, o principal fundamento de legitimidade aplicado neste contexto.

Entretanto, quando verifica-se, nesse contrato, o tratamento de categorias especiais de dados, tem de ser avaliado se esses dados constam das exceções do artigo 9.º do RGPD – cumprimento de uma obrigação legal ou exames médicos (alíneas b) e h) do n.º 2 do presente artigo).

Se seguir alguma dessas exceções, defendo a aplicação cumulativa do artigo 6.º e 9.º, n.º 2 do RGPD.

Exemplo:

O João celebra um contrato de trabalho com uma empresa do setor bancário e os seus dados pessoais são tratados para a finalidade contratual. Consta de uma cláusula do contrato o tratamento de dados biométricos para o controlo da assiduidade.

Como se trata de uma categoria especial de dados e constitui uma das exceções do artigo 9.º do RGPD, por se tratar do cumprimento de uma obrigação legal, é aplicado cumulativamente o artigo 6.º e o artigo 9.º, n.º 2 do RGPD.

Simplesmente, esta aplicação vem reforçar o tratamento de dados neste contexto, sobretudo por envolverem categorias especiais de dados, que precisam de uma maior proteção face aos restantes. No entanto, parece não haver consenso entre as várias autoridades de controlo da UE.

O ICO defende essa aplicação afirmando a necessidade de identificar o fundamento de legitimidade previsto no artigo 6.º do RGPD e a exceção do artigo 9.º do RGPD de modo a demonstrar conformidade para aplicar cumulativamente as duas normas, nos casos em que se verifique o tratamento de categorias especiais de dados⁷¹.

⁷¹ Disponível em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (acedido a 17/05/2019).

Porém, existem autoridades de controlo que defendem apenas a aplicação do artigo 6.º do RGPD, como é o caso da CNIL.

A CNIL publicou um documento⁷² em que estabelece o tratamento de dados pessoais para efeitos da gestão de recursos humanos, destacando, entre as várias matérias, os fundamentos de licitude.

Segundo o documento, as condições de licitude aplicadas no tratamento de dados pessoais neste contexto baseiam-se no consentimento, execução do contrato, cumprimento de uma obrigação legal e interesse legítimo (alíneas a), b), c) e f) do n.º 1 do art. 6.º do RGPD).

A tabela 1 do Anexo I demonstra as várias atividades de tratamento de dados pessoais que resultam da gestão de recursos humanos, seguido da sua finalidade e o fundamento de legitimidade aplicado. Esta tabela tem por objeto realçar as situações específicas de tratamento que decorrem dentro deste âmbito, por se tratar de uma área de grande complexidade que envolve todos os momentos que constituem a relação laboral, daí o alargamento das condições de licitude previstas no artigo 6.º do RGPD.

Em Portugal, a posição da CNPD carece de clarificação quanto à aplicação cumulativa das duas disposições. Neste sentido, o problema em questão tem de ser esclarecido pelo CEPD, porque, de outro modo, vai gerar insegurança jurídica na aplicação do RGPD e divergências de aplicação entre as autoridades de controlo dos vários Estados-Membros.

2.3 – OS PROCESSOS DE RECRUTAMENTO

2.3.1 – TRATAMENTO DE DADOS PESSOAIS

⁷² *Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par organismes ou publics aux fins de gestion du personnel.* Disponível em <https://www.cnil.fr/sites/default/files/atoms/files/referentiel-grh.pdf> (acedido a 02/08/2019).

Com a evolução tecnológica nas últimas décadas, as modalidades de recrutamento sofreram inúmeras alterações, passando do papel através do CV para as redes sociais profissionais, como o *LinkedIn*.

Atualmente, os candidatos recorrem cada vez mais a perfis em redes sociais e não tanto ao CV “tradicional”, com o objetivo de demonstrar o seu talento de forma ampla e pública às empresas.

Neste sentido, a entrada em vigor do RGPD impactou significativamente as atividades dos departamentos de recursos humanos e das empresas de trabalho temporário dada a grande quantidade de dados pessoais que armazenam e processam relativamente a candidatos, trabalhadores, ex-trabalhadores e clientes nas suas bases de dados.

No entanto, os RH estão sempre à procura de novos talentos para fazer face às necessidades das empresas. Por isso, acedem com grande facilidade às redes sociais, sobretudo de possíveis candidatos. Mas devem ter em conta o tipo de perfil que o candidato apresenta, designadamente se é público ou profissional.

Em Portugal, é muito comum os recrutadores, durante o processo, consultarem os perfis públicos dos candidatos, com o intuito de conhecer melhor a pessoa que estão prestes a contratar.

Entretanto, tem aumentado o número de empresas que recorrem a sistemas automatizados para apoiar os processos de recrutamento. Estes consistem em ferramentas de inteligência artificial com o objeto de criar um perfil comportamental, associado à personalidade do candidato através da análise das redes sociais, antes mesmo de verificar detalhadamente o CV – como o caso da *DeepSense*⁷³.

O RGPD prevê um enquadramento para estas práticas através do artigo 22.º e considerando 71⁷⁴. No entanto, estas práticas apresentam incompatibilidades face ao RGPD pela forma como atuam, conduzindo à aplicação de coimas (n.º 5 do art. 83.º do

⁷³ Disponível em <https://expresso.pt/dossies/diario/2018-10-08-Empresas-que-vigiem-nas-redes-sociais-candidatos-a-emprego-violam-a-lei#gs.4l61t0> (acedido a 11/04/2019).

⁷⁴ Ver ponto 1.3.4, p. 36 - 37.

RGPD) por as empresas não agirem em conformidade. Ou seja, além de o candidato não ter conhecimento do tratamento dos seus dados nem ter dado o consentimento para tal, pode gerar situações de discriminação na escolha do candidato – por exemplo, não contratarem determinado candidato só pelo facto de pertencer a um partido político.

Portanto, é fundamental informar os candidatos antes de iniciar o processo de recolha para o tratamento de dados pessoais, respeitando assim, o princípio da licitude, lealdade e transparência (art. 5.º do RGPD).

Conforme o Parecer 2/2017, os empregadores podem considerar a inspeção de perfis sociais públicos de possíveis candidatos, justificando essa inspeção durante o processo de recrutamento. Mas é necessário um fundamento de legitimidade, como o interesse legítimo, para efetuar o tratamento dos dados. Assim, antes de o empregador verificar determinado perfil, deve ter em atenção se este apresenta carácter profissional ou pessoal, por ser um indicador para a admissibilidade jurídica dos dados⁷⁵.

Sendo assim, apenas podem ser recolhidos os dados necessários para o processo de recrutamento do candidato. Um bom exemplo desse método é o *LinkedIn*.

O *LinkedIn* é uma plataforma profissional com o intuito de os utilizadores apresentarem as suas qualificações - como o CV - de forma a serem consultados por empresas que procurem novos talentos. Mas também pode ser visto como uma forma de promover a própria marca profissional.

As empresas, sobretudo de trabalho temporário, recorrem cada vez mais a esta ferramenta pelo facto de apresentar a informação essencial e relevante dos candidatos.

Assim, quando um utilizador se candidata, os dados recolhidos para tratamento serão os que constam do perfil. Consequentemente, quando chamado para uma entrevista, preenche um formulário de candidatura onde coloca a informação adicional que não consta no perfil.

Para além das utilidades que as novas tecnologias trouxeram para os processos de recrutamento, o CV ainda é muito utilizado por ser o “cartão de entrada” para o

⁷⁵ Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 13.

mercado de trabalho e apresentar todo o histórico profissional e académico de um indivíduo. Logo, quando um candidato utiliza este método, envia o CV para a empresa que publicou a vaga ou preenche um formulário *online* através do *website*, prosseguindo para uma entrevista caso seja selecionado, passando pelo mesmo processo verificado através do recrutamento pelo *LinkedIn*.

Os métodos de recolha são diferentes, mas o restante processo é igual em ambos os casos.

Todavia, após a entrada em vigor do RGPD, os RH persistem, em grande parte, em não transmitir a informação relativa à finalidade do tratamento dos dados, incumprindo os artigos 13.º e 14.º do RGPD e as orientações do Parecer 2/2017. O mesmo acontece quando o candidato vai a uma entrevista e o recrutador não o informa sobre o tratamento dos dados pessoais, ou então apresenta o modelo padrão de colocar a “cruz no quadrado” no formulário de candidatura, transmitindo por vezes, a informação em letras minúsculas de forma a dificultar a leitura e compreensão do consentimento para o tratamento dos dados.

Ao contrário do que acontece nos processos de recrutamento através de plataformas *online*, o CV contém alguns dados de carácter pessoal, que, apesar dos avisos por parte de especialistas, ainda ocorrem com alguma regularidade, como o exemplo do número de identificação fiscal e do cartão de cidadão.

Apesar de muitos dos dados contidos nas bases de dados serem obrigatórios durante o processo, existem informações que poderão ser minimizadas e/ou retiradas, como a morada completa, a nacionalidade e o estado civil. Isto porque, para além de ser irrelevante, à partida, é alvo de tratamento. Só quando ocorre a celebração do contrato é que estes dados se tornam importantes, sobretudo, para efeitos de processamento salarial.

Quando termina o processo de recrutamento⁷⁶ e a vaga é preenchida por outro candidato, todos os dados recolhidos durante o processo devem ser eliminados⁷⁷. Porém, é muito recorrente as empresas conservarem os dados dos candidatos com o intuito de estes poderem ser chamados quando surgir uma vaga similar à qual se candidataram anteriormente.

Deste modo, o titular deve ser informado dessa situação, dando a possibilidade de consentir ou opor-se a esse tratamento, caso pretenda a eliminação dos seus dados pessoais⁷⁸.

2.3.2 – PERÍODO DE CONSERVAÇÃO DOS CV’S

Apesar de não existir um limite específico relativo ao período de conservação⁷⁹ dos dados pessoais dos candidatos, a maioria das empresas conserva os dados durante o período de um ano⁸⁰, justificado com a abertura de vagas similares durante esse intervalo. Quando esse limite é ultrapassado, por norma, todos os dados associados ao candidato são eliminados.

Antes da entrada em vigor do RGPD, era recorrente as empresas assumirem o consentimento tácito dos candidatos relativamente à recolha e tratamento dos dados para efeitos de recrutamento e seleção⁸¹.

⁷⁶ As empresas têm de manter, por um período de cinco anos, o registo dos processos de recrutamento efetuados (art. 32.º do CT).

⁷⁷ Ponto 13.2 da Recomendação CM/Rec (2015) 5 do Comité aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral. Disponível em https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (acedido a 11/01/2019).

⁷⁸ *Ibidem*.

⁷⁹ O n.º 1 do artigo 21.º da Lei n.º 58/2019 prevê a fixação do prazo de conservação dos dados através de normal legal ou regulamentar e, na falta desta, o que se revelar necessário para a prossecução da finalidade.

⁸⁰ A CNPD tem defendido que os dados pessoais dos candidatos desatualizam até ao fim de um ano a contar desde a data da recolha. Nesse sentido, as empresas estipularam o prazo de um ano. Disponível em <https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/> (acedido a 22/01/2019).

⁸¹ Disponível em <https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/> (acedido a 22/01/2019).

Desde então, o cenário alterou-se. Além do consentimento apresentar uma definição mais exigente⁸², o titular tem um maior controlo sobre os seus dados pessoais (considerando 7 do RGPD), podendo exercer diversos direitos, como o direito de acesso (art. 15.º do RGPD)⁸³. Porém, o período de conservação não sofreu alterações.

No entanto, quando é iniciado o processo de recrutamento, o candidato tem de dar o consentimento explícito para o tratamento dos dados⁸⁴, sendo, nesse momento, informado do período de conservação (al. a) do n.º 2 do art. 13.º do RGPD).

Caso o candidato não pretenda que o seu CV permaneça na base de dados, se não preencher a vaga pretendida, pode opor-se ao tratamento dos dados (n.º 1 do art. 21.º do RGPD).

Porém, a finalidade para a conservação nem sempre é utilizada pelas empresas. Apesar de os RH mencionarem a possibilidade de chamar os candidatos caso abra uma vaga similar, isso nem sempre acontece. A vaga pode abrir, mas não informam os titulares que permitiram a conservação dos dados, originando bases de dados extensas e desatualizadas, dificultando o acesso devido à grande quantidade de dados armazenados que acabam por ser inúteis.

De forma a que esta situação não ocorra, facilitando o acesso e revisão dos dados pessoais dos candidatos, sugiro a seguinte alteração dos prazos de conservação nas duas modalidades de candidatura.

⁸² O legislador europeu desenhou a definição de consentimento de uma forma muito exigente, de modo a produzir uma manifestação de vontade, livre, específica, informada e explícita através de uma declaração ou ato positivo inequívoco (n.º 11 do art. 4.º e considerando 32 do RGPD).

⁸³ Apesar de os direitos do titular se encontrarem previstos na Diretiva, não eram de todo aplicados, devido ao seu desconhecimento por parte dos titulares.

⁸⁴ Disponível em <https://múltiplos.itpeers.com/2018/05/08/rgpd-gestao-de-recursos-humanos/> (acedido a 22/01/2019).

Vagas abertas	Candidatura espontânea
Período de conservação de seis meses. Depois de ultrapassado esse limite, os dados pessoais são excluídos da base de dados.	Período de conservação de três a seis meses. Os dados pessoais são excluídos assim que o limite máximo seja ultrapassado. Durante esse intervalo é feita uma triagem, selecionando os CV's que apresentem o <i>know-how</i> adequado para preencher as vagas que possam abrir futuramente.

Esta medida incide na redução do período de conservação em ambos os casos, pelo facto de o CV se desatualizar com grande facilidade. Basta um candidato frequentar um curso, aprender uma língua estrangeira ou mudar de residência para que esse CV apresente dados desatualizados.

Assim, respeitando este princípio, o prazo deve ser limitado ao mínimo, assegurando que os dados sejam conservados apenas durante o período considerado necessário para a finalidade em que incide o tratamento (considerando 39 do RGPD).

Desta forma, as bases de dados irão incluir apenas CV's atualizados, respeitantes aos candidatos que permitiram a conservação dos mesmos, tornando-se mais leves e fáceis de aceder, apresentando apenas os dados necessários, respeitando assim, os princípios da minimização⁸⁵ e da exatidão.

Ao aplicar o princípio da minimização, é necessário ter em conta a proteção de dados desde a conceção e por defeito. Isto porque, no momento em que são definidos os meios e/ou o próprio tratamento dos dados, devem ser consideradas as medidas técnicas e organizativas adequadas de forma a aplicar os princípios da proteção de dados, como o caso da minimização (n.º 1 do art. 25.º do RGPD). Assim, com a transformação que as bases de dados possam sofrer, através da possível aplicação de um novo prazo, estas medidas serão tidas em conta de forma a assegurar que os dados tratados são necessários para aquela finalidade específica (n.º 2 do art. 25.º do RGPD).

⁸⁵ Segundo este princípio, os dados são adequados, pertinentes e limitados para a finalidade em que os mesmos são tratados (art. 5.º, n.º 1, al. c) do RGPD).

Devido a esta particularidade, e dependendo do momento em que o candidato é chamado para entrevista, existe a possibilidade dos dados de que a empresa dispõe se encontrarem incompletos. Porventura, o titular tem o direito de os retificar (art. 16.º do RGPD) de modo a atualizá-los⁸⁶. Mas também pode exercer o direito ao apagamento, caso não pretenda ter mais os seus dados conservados, por estes deixarem de ser necessários para a finalidade que motivou a recolha ou tratamento (al. a) do n.º 1 do art. 17.º do RGPD).

2.4 – O CONSENTIMENTO NO CONTRATO DE TRABALHO

Segundo o n.º 11 do artigo 4.º do RGPD, o consentimento é uma manifestação de vontade, livre, específica, informada e explícita, em que o titular aceita o tratamento dos dados que lhe digam respeito, através de uma declaração ou ato positivo inequívoco. Constitui um dos fundamentos de licitude para o tratamento de dados pessoais previsto no artigo 6.º do RGPD.

No entanto, só constitui um fundamento de legitimidade válido quando é oferecido ao titular uma verdadeira opção de aceitar ou recusar, sem sair prejudicado caso recuse consentir o tratamento⁸⁷. Neste sentido, o consentimento deve ser uma decisão reversível⁸⁸, de forma a que o titular possa ter um maior controlo sobre os seus dados relativamente à decisão que tome quanto ao seu tratamento.

São vários os casos em que o consentimento é considerado inválido⁸⁹. Estas situações devem-se à presença de algum elemento que pressione ou influencie o titular, impedindo-o de exercer livremente a sua escolha.

⁸⁶ O direito de retificação segue o princípio de exatidão, devido ao facto de os dados serem exatos e atualizados sempre que for necessário (art. 5.º, n.º 1, al. d) do RGPD).

⁸⁷ Grupo de Trabalho do Artigo 29.º - *Orientações relativas ao consentimento na aceção do Regulamento 2016/679*, adotadas em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018, p. 3.

⁸⁸ O responsável pelo tratamento tem de demonstrar a possibilidade de recusa ou retirada do consentimento sem que o titular dos dados seja prejudicado (considerando 42 do RGPD).

⁸⁹ Um exemplo claro de consentimento inválido é o que se verifica quando utilizamos uma aplicação de *smartphone* para editar fotografias. Para utilizar a aplicação, é estritamente necessário ativar o GPS, como também a recolha de dados para efeitos publicitários. Apesar de o GPS e a publicidade não constituírem a finalidade para

No contexto laboral, existe uma enorme discussão sobre se o consentimento constitui, ou não, um fundamento de legitimidade para o tratamento dos dados pessoais dos trabalhadores. Como prevê o n.º 3 do artigo 28.º da Lei n.º 58/2019⁹⁰, o consentimento não constitui um fundamento de legitimidade válido para o tratamento dos dados pessoais, se esse tratamento abranger a alínea b) do n.º 1 do artigo 6.º do RGPD (alínea b) do n.º 3 do presente artigo).

Como prevê o artigo 11.º do CT, o trabalhador é obrigado a prestar a sua atividade sob a autoridade e direção do empregador, recebendo em contrapartida a remuneração baseada no exercício dessa função.

Portanto, o trabalhador apresenta uma dependência económica face ao empregador, pela subordinação jurídica resultante da relação laboral, o que leva à situação de desequilíbrio relativamente ao consentimento do tratamento dos dados⁹¹. Assim, é improvável que o trabalhador possa recusar o consentimento sem que exista um risco, caso queira tomar essa decisão⁹².

O Parecer 2/2017 veio reforçar essa questão, demonstrando a rara posição em que se encontra o trabalhador de dar, recusar ou revogar livremente o consentimento, devido à dependência económica que resulta da relação laboral, dando origem ao desequilíbrio de poderes. Assim, os trabalhadores apenas podem dar livre consentimento em situações excecionais, quando não ocorram consequências relativas à aceitação ou rejeição da oferta em questão⁹³.

a qual se destina a aplicação, esta só funciona na sua plenitude se o utilizador der o consentimento para estes efeitos, demonstrando que o consentimento não pode ser livre. (Ver Grupo de Trabalho do Artigo 29.º - Cit. 86, p. 6).

⁹⁰ A CNPD deliberou desaplicar a alínea a) do n.º 3 do presente artigo, por não apresentar uma medida legislativa adequada que salvaguarde a dignidade, os direitos fundamentais e o interesse legítimo do trabalhador, não cumprindo com os requisitos exigidos na alínea b) do n.º 2 do artigo 9.º e do n.º 2 do artigo 88.º do RGPD. Isto deve-se, pela a norma em questão, restringir excessivamente a relevância do consentimento do trabalhador, conduzindo a uma restrição injustificada e desproporcionada da alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD. (Deliberação 2019/494 sobre a desaplicação de normas da Lei n.º 58/2019, de 8 de agosto – N.º 4, p. 5).

⁹¹ No passado, verificava-se um uso e abuso do consentimento como fundamento de licitude, apesar de, na maior parte dos casos, não haver realmente consentimento devido à dependência económica resultante da relação laboral.

⁹² O G29 considera esta questão problemática, no sentido em que o empregador procede ao tratamento de dados pessoais de candidatas e trabalhadores baseado no consentimento por este não ser dado livremente. (Ver Grupo de Trabalho do Artigo 29.º - Cit. 86, p. 7).

⁹³ Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 28.

Dado estes factos, o consentimento não pode constituir um fundamento jurídico válido (considerando 43 do RGPD), restringindo, desta forma, os fundamentos de licitude válidos para o tratamento dos dados pessoais caso se verifique qualquer desequilíbrio na relação entre as partes⁹⁴.

Antes da entrada em vigor do RGPD, as operações de tratamento de dados baseavam-se na obtenção do consentimento dos trabalhadores através de uma cláusula de tratamento de dados pessoais prevista no contrato de trabalho. Assim, o trabalhador expressamente autorizava e consentia ao empregador o tratamento dos dados no âmbito da relação laboral⁹⁵.

Após a entrada em vigor, ocorreu a necessidade de informar novamente os trabalhadores relativamente aos seus direitos enquanto titulares (artigos 13.º e 14.º do RGPD) e a finalidade do tratamento dos dados. Esta informação foi transmitida, ao longo do período de transição, através da revisão de políticas internas de privacidade, contratos de trabalho já celebrados e adoção de novas cláusulas de tratamento de dados nos contratos de trabalho a serem celebrados futuramente⁹⁶.

Este conjunto de obrigações legais é imposto ao empregador, de forma a que sejam adotados mecanismos internos e eficazes de controlo e cumprimento com as normas legais estipuladas, evitando assim as sanções previstas pelo incumprimento do RGPD⁹⁷.

2.5 – MONITORIZAÇÃO DOS TRABALHADORES DENTRO E FORA DO LOCAL DE TRABALHO

2.5.1 – CONSIDERAÇÕES GERAIS

Com a crescente utilização de novas tecnologias no local de trabalho, as empresas foram implementando novos instrumentos e métodos para facilitar o desempenho dos

⁹⁴ HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – Cit. 45, p. 21.

⁹⁵ *Ibidem*.

⁹⁶ *Idem*. p. 27.

⁹⁷ *Ibidem*.

trabalhadores. Consequentemente, surgiram novas formas de controle por parte do empregador em relação aos trabalhadores.

Assim, nasceram técnicas com o objetivo de monitorizar os trabalhadores tanto dentro como fora do local do trabalho⁹⁸. Todavia, estas práticas são vistas como a principal ameaça contra a privacidade dos trabalhadores⁹⁹, podendo, em alguns casos, ser intrusivas se não existirem limites ao tratamento e transparência por parte do empregador.

Deste modo, tem suscitado alguns riscos que põem em causa a vida íntima e privada do trabalhador.

Em primeiro lugar, a monitorização das comunicações apresenta um efeito dissuasor sobre os trabalhadores na organização do trabalho e comunicação confidencial, por conduzir à alteração de comportamentos, dada a pressão exercida para que os trabalhadores estejam em conformidade, comprometendo a sua privacidade. Isto deve-se ao aumento de dados pessoais gerados neste contexto e a abertura a novas técnicas de análise que resultam na monitorização dos padrões de comportamento e desempenho do trabalhador¹⁰⁰.

No entanto, os trabalhadores podem nem ter conhecimento das tecnologias de monitorização que estão a ser aplicadas, bem como dos dados pessoais objeto de tratamento¹⁰¹.

Em segundo lugar, o surgimento de técnicas de monitorização fora do local de trabalho merece um especial enfoque, por estas colidirem com a esfera privada do trabalhador, pondo em causa a sua privacidade através da recolha de dados que correspondem somente à sua vida íntima e privada quando utiliza dispositivos e/ou veículos disponibilizados pelo empregador.

⁹⁸ Essa monitorização apresenta diversas formas como a vigilância das comunicações eletrónicas, sistemas de geolocalização nas viaturas da empresa, aparecimento de novas modalidades de trabalho, entre outros.

⁹⁹ Apesar do direito à privacidade e direito da proteção de dados estarem relacionados, são direitos distintos. (Ver ponto 1.2, p. 20).

¹⁰⁰ Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 11 – 12.

¹⁰¹ *Idem*. p. 11.

O mesmo sucede com o aparecimento de novas modalidades de trabalho. As tecnologias utilizadas por estes meios podem representar um risco, dado o alargamento ao ambiente doméstico do trabalhador quando utiliza dispositivos com essa tecnologia¹⁰². Esta situação verifica-se, sobretudo, no regime de teletrabalho.

Não obstante, a monitorização pode apresentar um interesse legítimo para o empregador (al. f) do n.º 1 do art. 6.º do RGPD). Neste sentido, a finalidade do tratamento deve ser legítima, tal como o método e a tecnologia utilizada durante o seu tratamento, sendo este proporcional às necessidades da empresa.

O Parecer 2/2017 sintetiza quais os riscos associados à utilização de novas tecnologias, realçando a importância de realizar uma avaliação de proporcionalidade nos cenários em que as novas tecnologias são aplicadas¹⁰³.

No entanto, as empresas foram-se deparando com diversos cenários, em que é necessário realizar uma AIPD, quando a utilização das novas tecnologias implique um elevado risco para os direitos e liberdades das pessoas singulares (art. 35.º do RGPD).

O mesmo acontece quando o empregador disponibiliza ao trabalhador vários dispositivos para realizar as suas atividades, aplicando técnicas de proteção de dados desde a conceção e por defeito (art. 25.º do RGPD).

O tratamento de dados biométricos e o regime do teletrabalho são dois dos cenários, no âmbito laboral, em que se verifica o risco associado à utilização de novas tecnologias, por parte do trabalhador.

2.5.2 – DADOS BIOMÉTRICOS

Os dados biométricos são os dados pessoais relativos às características físicas, fisiológicas ou comportamentais de um indivíduo, com o intuito de confirmar a sua identidade única (n.º 14 do art. 4.º do RGPD). São constituídos por um conjunto de

¹⁰² *Idem.* p. 20.

¹⁰³ *Idem.* p. 5.

diferentes técnicas de reconhecimento como impressões digitais, geometria da mão ou da face, padrão da íris ou retina.

As empresas recorrem cada vez mais a sistemas que utilizam dados biométricos, de forma a controlar a atividade dos trabalhadores relativamente à assiduidade, pontualidade e acessos, tornando-se o método mais comum e de maior aplicação relativamente à monitorização dos trabalhadores no local de trabalho¹⁰⁴.

Por um lado, estes sistemas podem ser vistos como sistemas altamente invasivos, devido à finalidade com que o dado pessoal é utilizado e os riscos que apresenta para o próprio trabalhador: discriminação, cruzamento com outros sistemas, falta de fiabilidade e efeitos na esfera pessoal quando ocorra falsificação ou usurpação da característica biométrica utilizada¹⁰⁵.

Mas, por outro lado, apresentam vantagens em relação aos sistemas tradicionais, pelo facto da informação de acesso corresponder unicamente a uma só pessoa, tornando a perda ou a apropriação por terceiros impossível de concretizar.

Assim, é considerado um sistema confiável, preciso e seguro, por não haver a necessidade de obter códigos ou chaves de identificação¹⁰⁶. Ou seja, o trabalhador detém uma chave única de acesso por esta se basear nas suas características físicas, fisiológicas ou comportamentais quando acede ao sistema.

Neste sentido, a finalidade do tratamento é a agilização da norma prevista no artigo 18.º do CT¹⁰⁷ e a integração de poderes de controlo por parte do responsável pelo tratamento¹⁰⁸, que incidem na fixação do horário de trabalho, controlo de assiduidade, registo do tempo de trabalho e controlo do trabalho suplementar¹⁰⁹.

Com a transição da Diretiva para o RGPD, ocorreram alterações relativamente à sua categorização e, posteriormente, ao tratamento dos dados.

¹⁰⁴ Orientações da CNPD - Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade, de 26 de fevereiro de 2004, considerando 1.

¹⁰⁵ Orientações da CNPD – Cit. 102, considerando 49.

¹⁰⁶ Orientações da CNPD – Cit. 102, considerando 2.

¹⁰⁷ O n.º 1 do artigo 18.º do CT encontra-se derogado devido à alteração estrutural prevista no considerando 89 do RGPD.

¹⁰⁸ Encontram-se previstos no artigo 202.º do CT e devem ser conservados por um período de 5 anos.

¹⁰⁹ Orientações da CNPD – Cit. 102, considerando 27.

Os dados biométricos passaram a fazer parte das categorias especiais de dados e, apesar do seu tratamento ser proibido por força do n.º 1 do artigo 9.º do RGPD, podem vir a ser tratados se constituírem o cumprimento de obrigações e exercício de direitos específicos da relação laboral (al. b) do n.º 2 do art. 9.º do RGPD) e execução do contrato (al. b) do n.º 1 do art. 6.º do RGPD), isto quando aplicado cumulativamente o artigo 6.º e 9.º, n.º 2 do RGPD. Nas situações em que é aplicado somente o artigo 6.º do RGPD, o fundamento de licitude utilizado é a execução do contrato.

O n.º 6 do artigo 28.º da Lei n.º 58/2019 também reforça a legitimidade do tratamento dos dados biométricos, sendo esta apenas legítima para o controlo de assiduidade e de acessos às instalações do empregador.

Por conseguinte, o consentimento é afastado como fundamento de legitimidade, dada a situação de desequilíbrio resultante da relação laboral¹¹⁰. De igual modo, não pode ser exercido, por parte do titular, o direito de se opor ao tratamento destes dados¹¹¹ por constituírem uma obrigação contratual.

Quando as empresas pretendem implementar estes sistemas, é necessário realizar uma AIPD antes de iniciar o tratamento, uma vez que a utilização de novas tecnologias é suscetível de implicar um risco elevado para os direitos e liberdades dos trabalhadores (n.º 1 do art. 35.º do RGPD) com o intuito de avaliar a probabilidade ou gravidade do risco tendo em conta a natureza, âmbito e as finalidades do tratamento (considerando 90 do RGPD).

O Regulamento 1/2018 da CNPD¹¹² faz essa referência, sobretudo quando o tratamento de dados biométricos afete pessoas vulneráveis, como é o caso dos trabalhadores¹¹³.

Além da AIPD, os sistemas de dados biométricos devem seguir as técnicas de proteção de dados desde a conceção e por defeito (art. 25.º do RGPD). Neste sentido, o responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios de

¹¹⁰ Orientações da CNPD – Cit. 102, considerando 35.

¹¹¹ Segundo o considerando 30, o titular dos dados pode, “em abstrato”, opor-se ao tratamento, mas é uma situação que irá depender de caso para caso. Porém, neste caso em concreto, não é possível que o titular se oponha ao tratamento dos dados biométricos. (Orientações da CNPD – Cit. 102, considerando 30).

¹¹² Ver *Regulamento 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados*.

¹¹³ Ver Grupo de Trabalho do Artigo 29.º - Cit. 43, critério 7.

tratamento, como da finalidade específica do mesmo, medidas técnicas e organizativas adequadas, com o intuito de serem aplicados os princípios da proteção de dados, seguindo assim, o princípio da minimização (n.º 1 do art. 25.º do RGPD).

O trabalhador deve ser informado quando o empregador pretenda implementar sistemas de dados biométricos na empresa. É fundamental ter o conhecimento da finalidade do tratamento dos dados, bem como da própria monitorização de forma a garantir que os direitos e deveres da relação laboral estão a ser respeitados.

2.5.3 – TELETRABALHO

Nos últimos anos, tem-se verificado um aumento de trabalhadores a prestar atividade laboral fora da empresa, mais concretamente no seu domicílio, passando este a ser o seu “novo” local de trabalho. O surgimento desta nova modalidade é o resultado do enfoque no processo científico e tecnológico de uma sociedade pós industrial – a sociedade da informação¹¹⁴.

O teletrabalho é considerado uma prestação laboral realizada com subordinação jurídica, fora das instalações da empresa, através do uso de tecnologias de informação e comunicação (art. 165.º do CT). Pressupõe, assim, dois pontos essenciais para a sua execução:

- I. O trabalhador tem de exercer funções fora das instalações da empresa, mantendo sempre contacto, de forma a apresentar o seu trabalho; e
- II. A utilização das TIC por ser o meio através do qual irá prestar a atividade laboral¹¹⁵.

¹¹⁴ AMADO, João Leal - *Contrato de Trabalho*, 4ª Edição. Coimbra: Coimbra Editora, 2014, p. 159.

¹¹⁵ JACINTO, José Moura - *Lições de Direito do Trabalho I: III Contrato de trabalho*. Lisboa: ISCSP, 2015, p. 23.

Portanto, as TIC utilizadas pelo trabalhador devem pertencer ao empregador que assegura as responsabilidades de instalação, manutenção e pagamento das despesas (n.º 1 do art. 168.º do CT), sendo essa uma das especificidades do teletrabalho.

Apesar de o teletrabalhador executar funções fora das instalações da empresa, tem os mesmos direitos e obrigações dos demais trabalhadores (art. 169.º do CT). Porém, esta modalidade apresenta algumas particularidades no seu exercício, tendo um enfoque especial no direito à privacidade¹¹⁶.

O teletrabalhador possui um direito à privacidade reforçado, pelo facto de a utilização das TIC poder conduzir a situações que comprometam a intimidade, descanso e repouso familiar do trabalhador. No entanto, o empregador deve respeitar a sua privacidade e proporcionar boas condições de trabalho (n.º 1 do art. 170.º do CT)¹¹⁷.

Ao entrarmos no campo do direito à privacidade do teletrabalhador, temos de ter em atenção as orientações do Parecer 2/2017 relativamente à monitorização do trabalhador nesta modalidade de trabalho.

Como a lei prevê, o empregador entrega ao trabalhador o equipamento necessário para desempenhar funções no seu domicílio e/ou à distância, de forma a que tenha o mesmo acesso à rede, sistemas e recursos, tal como se estivesse na empresa.

Apesar de a adesão a esta modalidade demonstrar um desenvolvimento positivo, apresenta um risco adicional para o empregador em relação às técnicas adequadas de utilização. Isto é, o trabalhador ao usar técnicas desadequadas, pode levar ao aumento do risco de acesso não autorizado, conduzindo à perda ou destruição de informações, como dados pessoais de trabalhadores ou clientes¹¹⁸.

¹¹⁶ *Idem.* p. 25.

¹¹⁷ Uma das obrigações do empregador consiste em visitar o domicílio do trabalhador com o objetivo de controlar a sua atividade laboral e os instrumentos de trabalho, num horário limitado - das 9 às 19 horas - com a presença do mesmo ou outra pessoa por ele designado (n.º 2 do art. 170.º do CT). Por ser caracterizada como uma norma excecional, deve ser articulada conjuntamente com o artigo 168.º do CT. (Ver JACINTO, José Moura - Cit. 113, p. 25).

¹¹⁸ Grupo de Trabalho do Artigo 29.º - Cit. 60, p. 20.

Segundo o RGPD, a segurança dos dados é fundamental; por isso, este diploma impõe regras mais exigentes aos responsáveis pelo tratamento e subcontratantes para que os dados pessoais se encontrem em segurança (art. 32.º do RGPD).

As soluções para atenuar os riscos ligados a esta modalidade devem envolver uma abordagem proporcional e não excessiva, de forma a manter a fronteira entre a utilização privada e profissional dos instrumentos de trabalho¹¹⁹.

Neste sentido, o Parecer 2/2017 identifica dentro dos nove cenários de tratamento de dados no contexto laboral, nos quais as novas tecnologias podem suscitar potenciais riscos para a sua privacidade, a monitorização através da utilização das TIC fora do local de trabalho; ou seja, o teletrabalho.

Como o teletrabalho requer a utilização das TIC disponibilizadas pelo empregador, este deve seguir a proteção de dados desde a conceção e por defeito. Ou seja, quando o empregador entrega dispositivos ao trabalhador para desempenhar funções no seu domicílio, estes devem, no momento da definição dos meios e no próprio tratamento, apresentar medidas técnicas e organizativas adequadas que demonstrem conformidade com as regras de proteção de dados, incidindo sobretudo nos dados que sejam realmente necessários para a finalidade específica do tratamento (art. 25º do RGPD).

Desta forma, o direito à privacidade do teletrabalhador encontra-se resguardado, uma vez que a obrigação das técnicas de proteção de dados desde a conceção e por defeito incide apenas nos dados alvo de tratamento, aplicando-se à quantidade de dados pessoais recolhidos, à extensão do tratamento, ao prazo de conservação e à sua acessibilidade (n.º 2 do art. 25.º do RGPD). Assim, a monitorização do teletrabalhador acaba por ter o objeto o seu próprio trabalho e não a sua vida íntima e privada. No entanto, os instrumentos de trabalho devem ser apenas utilizados para desempenhar o seu trabalho e não para utilização privada, de forma a que não seja posta em causa a sua intimidade.

¹¹⁹ *Ibidem*.

2.6 - SÍNTESE CONCLUSIVA

Ao longo do 2.º Capítulo foram investigadas as diferentes ocasiões em que se verifica o tratamento de dados pessoais de trabalhadores.

Partindo do princípio, o tratamento de dados pessoais neste contexto consiste no ciclo de vida do contrato de trabalho, sendo aplicada diversa legislação que vai depender do momento em que ocorre o tratamento dos dados.

Porém, devem ser tidos em conta os fundamentos de legitimidade no tratamento previstos nos artigos 6.º e 9.º, n.º 2 do RGPD, apesar de existirem divergências quanto à sua aplicação entre as várias autoridades de controlo europeias, incluindo a CNPD.

Ao entrar num dos momentos do ciclo de vida do contrato de trabalho, mais concretamente, no processo de recrutamento, verificamos o impacto que as novas tecnologias trouxeram ao criar novos métodos para recrutar talentos para as empresas, através das redes sociais profissionais. Não deixando de parte o método tradicional do CV.

Adicionalmente, as empresas recorrem, cada vez mais, a sistemas automatizados para auxiliar os processos de recrutamento, o que demonstra algumas incompatibilidades com o RGPD através do modo como atuam.

No entanto, é fundamental em qualquer das circunstâncias, seguir as diversas disposições do RGPD e as Orientações do G29 de forma a agirem em conformidade, sobretudo por ser uma situação específica no âmbito laboral.

Porém, nem todas as situações têm vindo a seguir essas regras como se verificou com o período de conservação dos CV's. Apesar dos recrutadores informarem a finalidade do tratamento dos dados pessoais dos candidatos, estes não são de todo respeitados, o que deverá conduzir a uma alteração dos períodos de conservação para uma maior e melhor aplicação do RGPD.

Entretanto, no momento de celebração do contrato de trabalho entre o trabalhador e empregador, é discutida a questão relativa ao facto de o consentimento constituir (ou

não) um fundamento de legitimidade para o tratamento dos dados pessoais. Todavia, neste contexto, é afastado como fundamento de licitude válido devido ao desequilíbrio de poderes que resultam da relação entre as partes.

Com o surgimento das novas tecnologias no local de trabalho, consequentemente, foram criados novos métodos de monitorizar os trabalhadores dentro e fora do local de trabalho, com o aparecimento de novas modalidades de trabalho e sistemas para controlar a assiduidade e o acesso dos trabalhadores, como o caso do regime do teletrabalho e os sistemas de dados biométricos para o controlo da assiduidade e acesso, respetivamente.

No entanto, apresentam alguns riscos que podem pôr em causa os direitos e liberdades dos trabalhadores, sendo necessário, em ambas as situações, realizar uma AIPD antes de iniciar as operações de tratamento dos dados pessoais e implementar técnicas de proteção de dados desde a conceção e por defeito às novas tecnologias inseridas no local de trabalho.

Em suma, o tratamento de dados pessoais nas relações laborais apresenta inúmeras situações específicas que irão depender do momento em que o titular se encontra no ciclo de vida do contrato de trabalho.

3.º CAPÍTULO – ESTUDO DE CASO

3.1 – INTRODUÇÃO

Após dois capítulos dedicados ao RGPD e à sua aplicação no contexto laboral, o terceiro e último capítulo constitui a componente prática de tudo o que foi analisado por meio do exercício dos direitos de titular de dados através da minha experiência enquanto candidata a emprego.

Durante os anos 2017 e 2018, candidatei-me a vários empregos, sobretudo estágios curriculares ou de verão, com o intuito de ganhar experiência profissional. Neste sentido, disponibilizei a várias empresas os meus dados pessoais enviando-lhes o meu CV.

No entanto, dado o desconhecimento nestas matérias na altura em que me candidatei, além de as próprias empresas não mencionarem a proteção de dados nas entrevistas e/ou formulários de candidatura, decidi contactar as empresas para as quais enviei o CV pedindo o acesso aos meus dados pessoais.

A partir do exercício deste direito irei analisar os seguintes aspetos:

- As políticas de privacidade estabelecidas pelas empresas;
- As respostas obtidas;
- As respostas não obtidas e as queixas apresentadas à autoridade de controlo nacional (CNPD); e
- O exercício de outros direitos do titular.

Desta forma, pretendo compreender como o RGPD está a ser aplicado em Portugal após o primeiro ano de vigência e se as empresas estão a agir em conformidade em relação ao exercício dos direitos do titular de dados.

3.2- POLÍTICAS DE PRIVACIDADE DAS EMPRESAS

Em primeiro lugar, como ponto de partida para a análise, selecionei as empresas para as quais tinha enviado CV – uma amostra de dez empresas - e antes de exercer o direito de acesso, elaborei uma pequena pesquisa através dos seus *websites*, para saber que informações disponibilizam ao público em geral, sobretudo aos titulares dos dados pessoais.

Neste sentido, reparei que todas as empresas, à exceção de uma, apresentam um *e-mail* específico para contactar o responsável pelo tratamento relativamente às políticas de privacidade e exercício de direitos do titular, mas apenas algumas disponibilizam o contacto do encarregado de proteção de dados.

Todas as empresas se descrevem como sendo o responsável pelo tratamento dos dados pessoais, por isso partilham dados aos (i) subcontratantes – sobretudo quando são empresas de trabalho temporário, (ii) a empresas pertencentes ao grupo, (iii) terceiros e (iv) autoridades públicas.

- **Finalidade do tratamento dos dados**

A finalidade invocada varia de empresa para empresa. As empresas de trabalho temporário tratam os dados para efeitos de recrutamento e seleção. As restantes são aquelas que não apresentam a finalidade por se tratarem, sobretudo, de empresas no setor do retalho e apenas divulgam políticas de privacidade associadas ao apoio ao cliente e não à gestão de carreiras.

Contudo, algumas referem que a finalidade está associada à informação necessária para o projeto, o que pode levar a questionar-me sobre o tipo de projeto a que o responsável pelo tratamento se refere, pondo em causa um possível exercício de direito, por exemplo de oposição ou apagamento dos dados.

- **Período de conservação**

Das dez empresas, apenas quatro indicam o período de conservação que vai desde um até quatro anos. A meu ver, longos períodos são altamente desnecessários pelo facto

de os dados desatualizarem com grande facilidade, pelo que defendo a aplicação até seis meses, nas duas modalidades de candidatura¹²⁰.

Apesar das restantes empresas não mencionarem o período de conservação, indicam que retém durante o tempo estritamente necessário, através do consentimento do titular¹²¹. Ou seja, novamente não sei ao certo através da informação disponibilizada *online*, do período de conservação dos dados, não respeitando os princípios impostos pelo RGPD, e em concreto o princípio da transparência.

Assim, estamos perante uma lacuna relativamente aos períodos de conservação dos dados pessoais.

- **Fundamentos de licitude no tratamento**

São poucas as empresas - apenas três em uma amostra de dez - que apresentam os fundamentos de licitude no tratamento dos dados pessoais.

Como se verificou no ponto 2.2, a CNPD apresenta divergências quanto à aplicação cumulativa dos artigos 6.º e 9.º, n.º 2 do RGPD. Porém, as empresas seguem os fundamentos de legitimidade previstos no artigo 6.º do RGPD. Apenas uma faz referência à aplicação cumulativa das disposições quando ocorre o tratamento de categorias especiais de dados.

- **Direitos do titular dos dados**

Todas as empresas mencionam os direitos inerentes ao titular dos dados (artigos 15.º e seguintes do RGPD). Apenas uma informa expressamente o direito de não ser avaliado com base em tratamento automático (art. 22.º do RGPD), por se tratar de uma empresa de trabalho temporário que recorre a sistemas automatizados para auxiliar os processos de recrutamento.

¹²⁰ Ver ponto 2.3.2, p. 58.

¹²¹ Quando um candidato preenche o formulário de candidatura num processo de recrutamento e seleção, dá o seu consentimento (ou não) para a conservação dos dados durante aquele período ou posteriormente ao mesmo.

3.3 – DIREITO DE ACESSO

Para que o titular possa exercer o direito de acesso, necessita de contactar o responsável pelo tratamento para obter, através do mesmo, os dados que lhe digam respeito.

Deste modo, enviei um *e-mail* para as empresas a que tinha concorrido exercendo o direito de aceder aos meus dados pessoais (art. 15.º do RGPD).

Numa amostra de dez empresas, apenas cinco responderam ao pedido em tempo útil estabelecido por lei – prazo de um mês a contar da data de receção do pedido (n.º 3 do art. 12.º do RGPD).

O que demonstra que grande parte das empresas responde ao exercício dos direitos do titular. No entanto, são várias aquelas que fogem à regra e respondem após o prazo, sem justificarem o atraso da resposta ao pedido efetuado.

Consequentemente, o atraso na resposta por parte do responsável pelo tratamento sem qualquer justificação e as respostas não obtidas, levaram-me a apresentar queixa à CNPD, uma vez que os direitos não estavam a ser exercidos em conformidade com o RGPD, como vamos verificar mais adiante.

Relativamente às respostas obtidas, deve ser feita a distinção entre o ano 2017 e 2018 por nesse período ter entrado em vigor o RGPD, trazendo inúmeras alterações no tratamento de dados pessoais.

A maioria das empresas a que tinha concorrido em 2017, indicaram que os dados tinham sido eliminados, não constando mais da base de dados, por ter ultrapassado o período de conservação estabelecido. Porém, uma das empresas apresentou uma resposta diferente.

Nesta situação em concreto, o período de conservação é de dois anos. Por conseguinte, os dados pessoais ainda constam da base de dados conduzindo ao apagamento dos dados como vamos ver no próximo ponto.

Já as que concorri em 2018, apenas fizeram referência aos dados que tinha disponibilizado para a candidatura - o CV e o formulário de candidatura *online* e em papel, nas quais fui chamada para entrevista.

Como prevê o n.º 1 do artigo 15.º do RGPD, o responsável pelo tratamento deve fornecer um conjunto de informações específicas para dar a conhecer ao titular o tratamento efetuado aos seus dados pessoais.

Todavia, os responsáveis pelo tratamento não transmitem essas informações, apesar de estar previsto na lei que o devem fazer, por ser uma das suas obrigações (n.º 1 do art. 12.º do RGPD).

Das dez empresas testadas, apenas uma referiu a finalidade do tratamento dos dados – recrutamento e seleção por se tratar de uma empresa de trabalho temporário.

As restantes informações não foram transmitidas pelo responsável pelo tratamento, apesar de se encontrar em grande parte das políticas de privacidade, o que não deixa de ser uma obrigação, porque o responsável pelo tratamento tem de transmitir essas informações quando é exercido este direito.

Neste sentido, verifico que o direito de acesso não é exercido na íntegra, pelo facto de os responsáveis pelo tratamento transmitirem apenas as informações que consideram necessárias para o seu exercício e não todo o conjunto ao qual eu, enquanto titular, devo ter acesso, demonstrando a falta de transparência exigida pelo RGPD - mesmo tendo requerido, no pedido de acesso, que pretendo obter as informações específicas previstas no n.º 1 do artigo 15.º do RGPD.

3.4 – DIREITO AO APAGAMENTO

Através do direito de acesso, o titular pode exercer outros direitos (artigos 16.º e seguintes do RGPD) por ter obtido do responsável pelo tratamento a confirmação dos seus dados e um conjunto de informações específicas como a finalidade do tratamento (n.º 1 do art. 15.º do RGPD).

Por se tratar de uma situação particular, optei por exercer o direito ao apagamento dos dados, após ter obtido o acesso aos meus dados pessoais.

No momento em que o RGPD estava prestes a entrar em vigor, fui contactada pelo responsável pelo tratamento com o intuito de dar o consentimento para o tratamento dos dados que tinha disponibilizado através do *website* da empresa, neste caso, de trabalho temporário. Como, na altura, não respondi ao pedido feito pelo responsável, o consentimento ficou sem efeito, deixando os dados de ser tratados.

Ao obter o pedido de acesso, o responsável pelo tratamento comunicou que os meus dados pessoais – contactos, número de identificação fiscal e CV – ainda constavam da base de dados, devido ao período de conservação praticado pela empresa (dois anos), mas não eram objeto de tratamento por não ter dado o consentimento no momento em que foi pedido, o que me deixou confusa.

Segundo o considerando 32 do RGPD, o silêncio, as opções pré-validadas e a omissão não devem constituir um consentimento. No entanto, dado o facto de não ter consentido o tratamento dos dados, estes deveriam ter sido eliminados no momento em que o responsável pelo tratamento não obteve resposta da minha parte. Deste modo, estamos perante uma contraordenação grave que pode levar a empresa a pagar uma multa por violar um dos princípios básicos do tratamento dos dados pessoais (al. a) do n.º 5 do art. 83.º do RGPD).

É uma situação que acaba por passar despercebida na maioria dos casos, pois os dados pessoais quando constam de uma base de dados, estão a ser alvo de tratamento, independentemente de o titular ter consentido ou não o respetivo tratamento, daí resultar a necessidade de eliminar os dados assim que o titular não consinta o tratamento dos mesmos.

Apesar desta situação, o exercício de apagamento dos dados torna-se mais simples, uma vez que os mesmos deixam de ser necessários para a finalidade que motivou a recolha ou o tratamento (al. a) do n.º 1 do art. 17.º do RGPD). Logo, o responsável pelo tratamento assume que pretendo eliminar os dados através da minha confirmação para esse efeito, ou caso não responda, eliminá-los mesma.

3.5 – CONSIDERAÇÕES FINAIS

Com o desenvolvimento do estudo de caso, confirmei a aplicação do RGPD por parte das empresas, para as quais tinha enviado o meu CV. Mas dada as circunstâncias da sua implementação abrupta, encontrei várias lacunas que devem ser corrigidas o mais breve possível antes que as empresas sejam sancionadas por não estarem a agir em conformidade com o RGPD.

Num primeiro momento, as empresas disponibilizam através dos seus *websites* as políticas de privacidade estabelecidas. Mas, grande parte, não transmite informações relativas à finalidade do tratamento dos dados e os respetivos períodos de conservação, não cumprindo, assim, o princípio da licitude, lealdade e transparência (al. a) do n.º 1 do art. 5.º do RGPD) e o princípio da conservação (alínea e) do n.º 1 do art. 5.º do RGPD).

Recai sobre o responsável pelo tratamento, a responsabilidade de aplicar os princípios¹²² impostos pelo RGPD (n.º 2 do art. 5.º do RGPD). Mas verifica-se o seu incumprimento pelo facto dos princípios não estarem a ser aplicados em grande parte das políticas de privacidade estabelecidas pelas empresas testadas.

No entanto, é necessário fazer uma avaliação das políticas de privacidade para compreender as falhas apresentadas, de modo a que estas sejam posteriormente alteradas para uma aplicação eficaz do Regulamento.

Para fazer face a essa situação, é fundamental que a equipa que desenvolveu as políticas de privacidade tenha conhecimentos em direito da proteção de dados pessoais, de forma a certificar que as informações transmitidas estão em conformidade. Neste sentido, é necessário fazer uma reestruturação das políticas para que estas respeitem os princípios estabelecidos pelo RGPD, de modo a partilhar a informação completa ao titular dos dados.

¹²² Segundo o princípio da transparência, qualquer informação destinada ao público ou ao titular dos dados deve ser concisa, de fácil acesso e compreensão com uma linguagem clara e simples (considerando 58 do RGPD).

Entretanto, os responsáveis pelo tratamento devem seguir rigorosamente os prazos definidos por lei e, quando não possam responder dentro do prazo, devem informar o titular como é exigido (n.º 3 do art. 12.º do RGPD), para evitar que sejam apresentadas reclamações à autoridade de controlo e, possivelmente sanções por incumprimento (al. b) do n.º 5 do art. 83.º do RGPD).

O exercício dos direitos do titular foi um bom exemplo para demonstrar se as empresas estão a agir em conformidade com o RGPD. Grande parte, demonstrou a sua aplicabilidade através das políticas de privacidade ao mencionar os direitos que o titular pode exercer relativamente ao tratamento dos seus dados. O mesmo não se verifica quando, na prática, o titular exerce um dos direitos e o responsável pelo tratamento não cumpre com as suas obrigações¹²³. Um exemplo claro dessa situação é o que ocorreu quando exerci o direito de acesso, em que apenas metade da amostra respondeu ao pedido.

Assim, coloco a seguinte questão:

- *Se o responsável pelo tratamento não responde ao pedido de acesso aos dados pessoais, como é que o titular pode exercer os demais direitos?*

Através do incumprimento desta obrigação, o titular pode apresentar queixa à autoridade de controlo de forma a expor a situação. Neste sentido, como não obtive qualquer tipo de resposta por parte dos responsáveis pelo tratamento das diferentes empresas dentro do limite estabelecido por lei, mesmo após enviar um segundo pedido de acesso, apresentei queixa à CNPD.

Quando um titular quer apresentar uma queixa à CNPD, é necessário descrever a situação que deu origem à mesma e indicar toda a informação sobre o caso para que a autoridade de controlo possa avaliar o ocorrido¹²⁴.

¹²³ O responsável pelo tratamento à luz da lei, não pode recusar a dar seguimento ao pedido do titular para exercer um dos direitos previstos nos termos dos artigos 15.º a 22.º do RGPD. Só nos casos em que não consegue identificar o titular dos dados (n.º 2 do art. 12.º do RGPD).

¹²⁴ A CNPD através do seu *website*, descreve como o titular dos dados pode apresentar uma queixa. Disponível em <https://www.cnpd.pt/bin/queixas/queixas.htm> (acedido a 08/06/2019).

Desta forma, apresentei as seguintes informações:

- I. Breve explicação da situação que me levou a exercer o direito ao acesso dos dados pessoais; e
- II. Indicação das empresas que não responderam ao pedido de acesso, apresentando como prova os *e-mails* que tinha enviado para as empresas em questão.

Após ter apresentado queixa, a CNPD contactou-me para informar que tinham aberto processos para averiguar a situação descrita, informando no fim, qual o resultado dos mesmos. Ou seja, sempre que ocorra uma situação desta natureza, o titular tem o direito de apresentar uma reclamação à autoridade de controlo, para que esta avalie a razão pela qual o responsável pelo tratamento não cumpriu com as suas obrigações face ao RGPD.

CONCLUSÃO

A aplicação do RGPD no seu primeiro ano de vigência não tem sido fácil, sobretudo quando falamos de relações laborais.

O tratamento de dados pessoais no contexto laboral remete para um conjunto de situações específicas que ocorrem durante o ciclo de vida do contrato de trabalho, interligando-se com a área que se responsabiliza pela recolha e processamento dos dados pessoais relativos a candidatos e trabalhadores – a gestão de recursos humanos.

Verificámos, ao longo da dissertação, que esse conjunto de situações específicas e com algumas particularidades de tratamento ainda são pouco reconhecidas, na sua generalidade, pelo facto destas matérias serem pouco exploradas no que toca ao direito da proteção de dados pessoais.

Atualmente, a realização de operações de tratamento de acordo com o Regulamento apresenta algumas dificuldades, por os atores envolvidos ainda não estarem totalmente familiarizados com a sua aplicação, contribuindo para as eventuais falhas como se verificou através do estudo de caso.

No entanto, a informação relativa ao tratamento de dados pessoais nas relações laborais encontra-se dispersa e desatualizada, sobretudo quando se trata de Orientações da CNPD. É uma situação que se deve, sobretudo, à implementação tardia da Lei n.º 58/2019 que apenas entrou em vigor a 9 de agosto de 2019. Ou seja, um ano após a entrada em vigor do RGPD, conduzindo as empresas a seguir indicações que ainda estavam associadas à Diretiva em algumas matérias.

Para além disso, a CNPD precisa de clarificar a sua posição relativamente à aplicação de várias disposições do RGPD, por estas traduzirem implicações no tratamento de dados pessoais, mais concretamente, no modo como os fundamentos de legitimidade do tratamento podem ser aplicados neste contexto. Refiro a importância deste elemento dado o tratamento de dados pessoais de trabalhadores apresentar uma grande complexidade devido às particularidades que vão surgindo nas relações laborais e que

devem ser asseguradas através de diversa legislação, sobretudo o RGPD e a Lei n.º 58/2019.

Em suma, gostaria de deixar algumas recomendações com o intuito de demonstrar o caminho que ainda temos de percorrer para ir ao encontro de uma aplicação eficaz e correta do RGPD no contexto laboral:

- I. A necessidade de atualizar a informação sobre o tratamento de dados pessoais nas relações laborais o mais breve possível, para que as empresas estejam em conformidade com o Regulamento. Esta informação deve ser feita através de Orientações e Regulamentos da CNPD, já que se encontra em vigor a Lei n.º 58/2019.

No entanto, para este efeito, sugiro a criação de um documento semelhante ao publicado pela CNIL, relativo ao tratamento de dados pessoais para efeitos da gestão de recursos humanos, com o objeto de organizar, num só documento, os tratamentos de dados efetuados neste âmbito.

- II. Investir na formação dos responsáveis pelo tratamento e subcontratantes para que estes tenham uma visão ampla das suas obrigações enquanto responsáveis pelo cumprimento das regras de proteção de dados, de modo a corrigir as falhas que têm apresentado até ao momento.

ANEXO I

Tabela 1 – Aplicação prática do tratamento de dados pessoais de trabalhadores para efeitos da gestão de recursos humanos¹²⁵

Atividades de tratamento	Finalidade	Fundamento de legitimidade
Recrutamento	Processo de recrutamento	Execução do contrato (medidas pré-contratuais); Interesse legítimo
	Criação de uma base de dados com os CV's dos candidatos	Consentimento; Interesse legítimo
Gestão administrativa do pessoal	Gestão da base de dados relativa aos trabalhadores	Execução do contrato; Interesse legítimo
	Realização de relatórios estatísticos ou de listas de trabalhadores para responder às necessidades da gestão administrativa	Interesse legítimo
	Gestão da estrutura interna organizacional	Interesse legítimo
	Gestão de <i>fringe benefits</i>	Execução de contrato
	Gestão de eleições no seio organizacional	Obrigações legais
	Gestão de reuniões de órgãos representativos de pessoal	Interesse legítimo; Obrigações legais
Gestão de remunerações e cumprimento de formalidades administrativas	Estabelecimento de remunerações, fornecimento de grelha salarial e declaração social nominativa	Obrigações legais; Execução do contrato

¹²⁵ Fonte: *Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par organismes ou publics aux fins de gestion du personnel*. Disponível em <https://www.cnil.fr/sites/default/files/atoms/files/referentiel-grh.pdf> (acedido a 19/08/2019).

Fornecimento de ferramentas de TI aos trabalhadores	Manutenção e monitorização da rede informática	Interesse legítimo
	Gestão da rede informática permitindo a definição de acessos a aplicativos e outras redes	Interesse legítimo
	Implementação de dispositivos para garantir a segurança e o bom funcionamento das redes e aplicativos	Interesse legítimo
	Gestão do <i>e-mail</i> profissional	Interesse legítimo
	Utilização da <i>intranet</i> para divulgar ou recolher dados da gestão administrativa	Execução do contrato (medidas pré-contratuais); Interesse legítimo
Organização do trabalho	Gestão de agendas profissionais	Execução do contrato
	Gestão das tarefas dos trabalhadores	Execução do contrato (medidas pré-contratuais); Interesse legítimo
Gestão de carreiras e de mobilidade	Avaliação de desempenho dos trabalhadores	Interesse legítimo; Execução do contrato
	Gestão de competências profissionais internas	Interesse legítimo
	Validação do certificado de competências profissionais	Obrigação legal
	Simulação de carreira	Interesse legítimo
	Gestão da mobilidade profissional	Execução do contrato (medidas pré-contratuais); Interesse legítimo
Formação	Acompanhamento de pedidos e de períodos de formação	Execução do contrato (medidas pré-contratuais); Interesse legítimo
	Organização de ações de formação	Execução do contrato (medidas pré-contratuais); Interesse legítimo

	Avaliação de competências adquiridas através da formação	Execução do contrato (medidas pré-contratuais); Interesse legítimo
Gestão da ação social	Gestão da ação social e cultural implementada pelo empregador, excluindo a saúde ocupacional, atividades de serviço social ou suporte psicológico	Interesse legítimo

BIBLIOGRAFIA

1) MONOGRAFIAS:

ABRANTES, José João - *Direitos fundamentais da pessoa humana no trabalho em especial, a reserva da intimidade da vida privada (algumas questões)*. Coimbra: Edições Almedina, 2014.

AMADO, João Leal - *Contrato de Trabalho*, 4ª Edição. Coimbra: Coimbra Editora, 2014.

CASTELLS, Manuel - *A era da informação: economia, sociedade e cultura*. In *A Sociedade em rede*, 3ª Edição. Lisboa: Fundação Calouste Gulbenkian, Volume 1, 2007.

FAZENDEIRO, Ana - *Regulamento geral sobre a proteção de dados*, 3ª edição. Coimbra: Edições Almedina, 2018.

DE HERT, Paul & LAMMERAN, Hans - *Protection of Personal Data in Work-related Relation – Study*. Brussels: European Parliament, 2013.

JACINTO, José Moura - *Lições de Direito do Trabalho 1: III Contrato de trabalho*. Lisboa: ISCSP, 2015.

MARQUES, Garcia e MARTINS, Lourenço - *Direito da Informática*. Coimbra: Edições Almedina, 2000.

MARTINEZ, Pedro Romano *et al.* - *Código do Trabalho Anotado*, 11º Edição. Coimbra: Edições Almedina, 2017.

PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.) - *Anuário da Proteção de Dados 2019*. Lisboa: CEDIS, 2019.

PINHEIRO, Alexandre Sousa (coord.) - *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018.

PINHEIRO, Alexandre Sousa - *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. Lisboa: AAFDL, 2015.

PRATA, Ana (coord.) - *Código Civil Anotado*. Coimbra: Edições Almedina, Volume 1, 2017.

SALDANHA, Nuno - *Novo Regulamento Geral da Protecção de Dados: O que é? A quem se aplica? Como implementar?*. Lisboa: FCA, 2018.

SANTOS, Carlos - *Protecção de Dados dos Trabalhadores*. Lisboa: Universidade Autónoma de Lisboa, 2015. Disponível em [repositorio.ual.pt/bitstream/11144/1856/1/Protecao de Dados dos Trabalhadores.pdf](http://repositorio.ual.pt/bitstream/11144/1856/1/Protecao_de_Dados_dos_Trabalhadores.pdf) (acedido a 15/02/2019).

VASCONCELOS, Pedro Pais de - *Protecção de dados pessoais e direito à privacidade*, In *Direito da sociedade de informação I*. Coimbra: Coimbra Editora, 1999.

VOIGT, Paul & VON DEM BUSSCHE, Axel - *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Switzerland: Springer International Publishing AG, 2017.

WERTHEIN, Jorge - *A Sociedade da informação e os seus desafios*. In *Ciência de Informação*. Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia, Volume 9, n.º 2, 2000. Disponível em <http://www.scielo.br/pdf/%0D/ci/v29n2/a09v29n2.pdf> (acedido a 02/07/2019).

2) **PUBLICAÇÕES, DOCUMENTOS, ORIENTAÇÕES E RECOMENDAÇÕES:**

Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa - *Manual da Legislação Europeia sobre a Protecção de Dados*. Luxemburgo: Serviço das Publicações da União Europeia, 2014.

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões «*Uma abordagem global da proteção de dados pessoais na União Europeia*», de 1 de novembro de 2010.

Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - *Estratégia para o Mercado Único Digital na Europa*, COM (2015) 192 final. Bruxelas, 6 de maio de 2015.

Deliberações da CNPD - *Deliberação 2019/494 sobre a desaplicação de normas da Lei n.º 58/2019*, de 8 de agosto.

European Union Agency for Fundamental Rights, Council of Europe - *Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union*, 2018.

Grupo de Trabalho do Artigo 29.º - *Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral*.

Grupo de Trabalho do Artigo 29.º - *Documento de trabalho de 2002 sobre a vigilância das comunicações eletrónicas no local de trabalho*.

Grupo de Trabalho do Artigo 29.º - *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, adotado em 16 de Fevereiro de 2010.

Grupo de Trabalho do Artigo 29.º - *Parecer 3/2010 sobre o princípio da responsabilidade*, adotado em 13 de julho de 2010.

Grupo de Trabalho do Artigo 29.º - *Parecer 3/2013 sobre a limitação da finalidade*, adotado em 2 de Abril de 2013.

Grupo de Trabalho do Artigo 29.º - *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*, adotado em 8 de junho de 2017.

Grupo de Trabalho do Artigo 29.º - *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, adotadas em 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017.

Grupo de Trabalho do Artigo 29.º - *Orientações relativas ao consentimento na aceção do Regulamento 2016/679*, adotadas em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018.

Nota técnica n.º 8 da Autoridade para as Condições de Trabalho - *Impacto do Regulamento Geral de Proteção de Dados nas Relações Laborais*. Disponível em [http://www.act.gov.pt/\(pt-PT\)/Publicacoes/Documents/Nota%20T%C3%A9cnica%20n%C2%BA%208%20%20%20Impacto%20do%20Regulamento%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20nas%20Rela%C3%A7%C3%B5es%20Laborais.pdf](http://www.act.gov.pt/(pt-PT)/Publicacoes/Documents/Nota%20T%C3%A9cnica%20n%C2%BA%208%20%20%20Impacto%20do%20Regulamento%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20nas%20Rela%C3%A7%C3%B5es%20Laborais.pdf) (acedido a 17/05/2019).

Orientações da CNPD - *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade*, de 26 de Fevereiro de 2004.

Recomendação CM/Rec (2015) 5 do Comité aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral. Disponível em https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (acedido a 11/01/2019).

Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par organismes ou publics aux fins de gestion du personnel. Disponível em <https://www.cnil.fr/sites/default/files/atoms/files/referentiel-grh.pdf> (acedido a 02/08/2019).

3) **LEGISLAÇÃO E JURISPRUDÊNCIA:**

Acórdão de 9 de Novembro de 2010, “*Volker und Schecke e Eifert*”, C-92/09 e C-93/09, ECLI:EU:C:2010:662.

Acórdão de 30 de maio de 2013, “*Worten*”, C 342/12, ECLI:EU:C:2013:355.

Acórdão de 13 de maio de 2014, “*Google Spain*”, C-131/12, ECLI:EU:C:2014:317.

Acórdão de 20 de dezembro de 2017, “*Nowak*”, C-434/16, ECLI:EU:C:2017:994.

Código Civil, Decreto-Lei n.º 47344 – Diário do Governo n.º 274/1966, Série I de 1966-11-25.

Constituição da República Portuguesa, Decreto de aprovação da Constituição – Diário da República n.º 86/1976, Série I de 1976-04-10.

Código do Trabalho, Lei n.º 7/2009 – Diário da República n.º 30/2009, Série I de 2009-02-12.

Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito aos tratamentos de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Regulamentos da CNPD - *Regulamento 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados*, de 16 de outubro de 2018.

4) **NOTÍCIAS E WEBSITES CONSULTADOS:**

BAIRRÃO, Isabel - Os dados dos seus colaboradores respeitam o RGPD?. INFORH. Disponível em <https://inforh.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/> (acedido a 22/01/2019).

Câmara do Comércio e Indústria de Ponta Delgada – Assuntos Europeus. Disponível em <http://ccipd.pt/faqs/assuntos-europeus/> (acedido a 26/06/2019).

Comissão Nacional de Proteção de Dados. Disponível em <https://www.cnpd.pt> (acedido a 30/06/2019).

European Court of Human Rights - European Convention on Human Rights. <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c> (acedido a 02/10/2018).

MATEUS, Cátia - Empresas que vigiem nas redes sociais candidatos a emprego violam a lei. Jornal Expresso. Disponível em <https://expresso.pt/dossies/diario/2018-10-08-Empresas-que-vigiem-nas-redes-sociais-candidatos-a-emprego-violam-a-lei#gs.4l61t0> (acedido a 11/04/2019).

Os fundamentos de legitimidade no tratamento segundo o ICO. Disponível em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (acedido a 17/05/2019).

ROCHA, Andreia - As principais implicações do RGPD na gestão de recursos humanos. Múltiplos. Disponível em <https://multiples.itpeers.com/2018/05/08/rgpd-gestao-de-recursos-humanos/> (acedido a 22/01/2019).

União Europeia - Regulamentos, diretivas e outros atos legislativos. Disponível em https://europa.eu/european-union/eu-law/legal-acts_pt (acedido a 26/06/2019).

ÍNDICE GERAL

Declaração Antiplágio.....	5
Declaração de Conformidade do Número de Caracteres.....	6
Agradecimentos	7
Modo de Citação e Outros Esclarecimentos.....	8
Lista de Abreviaturas.....	9
Resumo.....	11
<i>Abstract</i>	12
Introdução.....	13
1.º Capítulo - Proteção de Dados Pessoais na União Europeia.....	17
1.1– Evolução Histórica da Proteção de Dados Pessoais na União Europeia.....	17
1.2– A Proteção de Dados Pessoais na Ordem Jurídica Portuguesa.....	19
1.2.1 – A Constituição.....	20
1.2.2 – O Código Civil.....	21
1.2.3 – O Código do Trabalho.....	21
1.3– O RGPD.....	23
1.3.1 – Contexto de aprovação e objetivos.....	23
1.3.2 – Principais conceitos.....	25
1.3.3 – Princípios relativos ao tratamento de dados pessoais.....	29
1.3.4 – Direitos do titular de dados pessoais.....	34
1.3.5 – Os papéis do Responsável pelo tratamento e Subcontratante.....	40
1.3.6 – Avaliação de Impacto sobre a Proteção de Dados.....	43
1.3.7 – Autoridade de Controlo.....	45
2.º Capítulo - Tratamento de Dados Pessoais no Contexto Laboral.....	47
2.1 – Enquadramento.....	47
2.2 – Os fundamentos de licitude.....	49
2.3 – Os processos de recrutamento.....	53

2.3.1 – Tratamento de dados pessoais.....	53
2.3.2 – Período de conservação dos CV's.....	57
2.4 – O consentimento no contrato de trabalho.....	60
2.5 – Monitorização dos trabalhadores dentro e fora do local de trabalho.....	62
2.5.1 – Considerações gerais.....	62
2.5.2 – Dados biométricos.....	64
2.5.3 – Teletrabalho.....	67
2.6 – Síntese conclusiva.....	70
3.º Capítulo – Estudo de caso.....	72
3.1 – Introdução.....	72
3.2 – Políticas de privacidade das empresas.....	73
3.3 – Direito de acesso	75
3.4 – Direito ao apagamento.....	76
3.5 – Considerações finais.....	78
Conclusão.....	81
 Anexo I.....	 83
Bibliografia.....	86

Errata da Dissertação de Mestrado em Direito e Gestão

Este documento tem o objetivo de retificar alguns pontos que foram sugeridos pelo júri durante a defesa da dissertação de mestrado intitulada “A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral”, desenvolvida por Patrícia Andreia Batista e Santos.

Página	Linha	Onde se lê	Deve ler-se
19	11	...o direito à vida privada e familiar de todas as pessoas (art. 8.º do TFUE) e o direito à proteção dos dados pessoais que lhe digam respeito, sendo objeto de tratamento lícito para finalidades específicas com o consentimento da pessoa em causa, assegurando o direito de aceder aos seus dados e obter a respetiva retificação (art. 9.º do TFUE).	...o direito à vida privada e familiar de todas as pessoas (art. 7.º do CDFUE) e o direito à proteção dos dados pessoais que lhe digam respeito, sendo objeto de tratamento lícito para finalidades específicas com o consentimento da pessoa em causa, assegurando o direito de aceder aos seus dados e obter a respetiva retificação (art. 8.º do CDFUE).
25	Nota de rodapé	Ver Acórdão de 13 de maio de 2014, “ <i>Google Spain</i> ”, C-131/12, ECLI:EU:C:2014:317	Ver Acórdão de 13 de maio de 2014, “ <i>Google Spain</i> ”, C-131/12, ECLI:EU:C:2014:317, n.º 54
52	1	Se pensarmos de forma lógica, o artigo 6.º do RGPD prevê como fundamento de licitude a execução de um contrato. Ou seja, na generalidade, o artigo 6.º do RGPD é aplicado devido ao facto de a relação laboral resultar da celebração do contrato entre trabalhador e empregador, realçando o principal fundamento de legitimidade. Mas, quando se verifica nesse contrato o tratamento de categorias especiais de dados, temos de avaliar se esses dados constam das exceções do artigo 9.º do RGPD. Se constituírem o cumprimento de uma obrigação legal ou exames médicos, seguem essas exceções – aplicação cumulativa do artigo 6.º e 9.º, n.º 2 do RGPD.	Ao pensar de forma lógica, o artigo 6.º do RGPD prevê como fundamento de licitude a execução de um contrato. Ou seja, em regra geral, o artigo 6.º do RGPD é aplicado pelo facto da relação laboral traduzir na celebração do contrato entre trabalhador e empregador, destacando assim, o principal fundamento de legitimidade aplicado neste contexto. Entretanto, quando verifica-se, nesse contrato, o tratamento de categorias especiais de dados, tem de ser avaliado se esses dados constam das exceções do artigo 9.º do RGPD – cumprimento de uma obrigação legal ou exames médicos (alíneas b) e h) do n.º 2 do presente artigo). Se seguir alguma dessas exceções, defendo a aplicação cumulativa do artigo 6.º e 9.º, n.º 2 do RGPD.

57	Nota de rodapé		O n.º 1 do artigo 21.º da Lei n.º 58/2019 prevê a fixação do prazo de conservação dos dados através de normal legal ou regulamentar e, na falta desta, o que se revelar necessário para a prossecução da finalidade.
59	9	...respeitando assim, o princípio da minimização.	...respeitando assim, os princípios da minimização e da exatidão.
60	Nota de rodapé		A CNPD deliberou desaplicar a alínea a) do n.º 3 do presente artigo, por não apresentar uma medida legislativa adequada que salvaguarde a dignidade, os direitos fundamentais e o interesse legítimo do trabalhador, não cumprindo com os requisitos exigidos na alínea b) do n.º 2 do artigo 9.º e do n.º 2 do artigo 88.º do RGPD. Isto deve-se, pela a norma em questão, restringir excessivamente a relevância do consentimento do trabalhador, conduzindo a uma restrição injustificada e desproporcionada da alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD. (Deliberação 2019/494 sobre a desaplicação de normas da Lei n.º 58/2019, de 8 de agosto – N.º 4, p. 5).
65	20	...tratamento ser proibido por força do n.º 1 do art. 9.º do RGPD	...tratamento ser proibido por força do n.º 1 do artigo 9.º do RGPD (...) isto quando aplicado cumulativamente o artigo 6.º e 9.º, n.º 2 do RGPD. Nas situações em que é aplicado somente o artigo 6.º do RGPD, o fundamento de licitude utilizado é a execução do contrato.
78	9	...o princípio da licitude, lealdade e transparência (al. a) do n.º 1 do art. 5.º do RGPD).	...o princípio da licitude, lealdade e transparência (al. a) do n.º 1 do art. 5.º do RGPD) e o princípio da conservação (alínea e) do n.º 1 do art. 5.º do RGPD).